Réf : ET_SEC_INVNUMW

Investigation numérique

Méthodologie d'investigation sur OS Windows

Objectif

L'investigation numérique est une discipline indispensable à la qualification d'incidents de sécurité ainsi qu'à la remédiation de données ciblées.

L'objectif de ce cours est de vous familiariser avec les techniques et méthodologies d'investigation sur un environnement Windows, tout en développant la collecte de données spécifiques dites "artefacts".

Public	Durée estimée pour le suivi des modules indispensables
Informaticiens	Durée des vidéos : 5h28 Durée des TP : 8h00

Contenu pédagogique

Les modules indispensables

Présentation du cours

Cours	Ce module vous propose la consultation d'une vidéo d'une durée de 0h01.

- Présentation du cours

Etat de l'art de l'investigation numérique

Cours	Ce module vous propose la consultation d'une vidéo d'une durée de 0h21.

- Objectif du module
- Introduction et taxonomie
- Les différentes disciplines
- Signes de compromission (IOC)
- Méthodologie d'investigation
- Conclusion du module

Les fondamentaux Windows

Cours

Ce module vous propose la consultation d'une vidéo d'une durée de 1h13.

- Objectifs du module
- Structure des répertoires
- Séquence de boot
- Bases de registres
- Logs et événements
- Variables d'environnement
- Services
- Volume Shadow Copy Service
- Démonstration - Montage d'un volume VSS
- Fondamentaux disque et système NTFS
- Démonstration - Analyse d'un disque avec Active@ Disk Editor
- Énoncé du TP - Analyse d'un disque avec Active@ Disk Editor
- Énoncé du TP - Questionnaire

Collecte de données et artefacts

Cours

Ce module vous propose la consultation d'une vidéo d'une durée de 3h29.

- Objectifs du module
- Principe et imaging
- Les outils d'analyse
- Live Forensic
- Démonstration - Explication d'un script PowerShell Live Forensic
- Fichiers essentiels et $MFT
- Démonstration - Plan de travail, registres, extraction et analyse de la $MFT
- Artefacts Internet
- Démonstration - Les artefacts internet
- Artefacts d'exécution
- Démonstration - Les artefacts d'exécution
- Artefacts de fichiers/dossiers
- Démonstration - Les artefacts de fichiers/dossiers
- Artefacts réseau
- Démonstration - Les artefacts réseau
- Artefacts utilisateurs
- Démonstration - Les artefacts utilisateurs
- Artefacts USB
- Démonstration - Les artefacts USB
- Artefacts fichiers supprimés
- Démonstration - Les artefacts fichiers supprimés
- Spécificités Active Directory
- Énoncé du TP - Première investigation
- Démonstration - Autopsy
- Démonstration - Kape
- Énoncé du TP - Deuxième investigation
- Conclusion du module

Anti-Forensic

Cours

Ce module vous propose la consultation d'une vidéo d'une durée de 0h23.

- Objectifs du module
- Principes de l'anti-forensic
- Les différents outils et techniques
- Démonstration - Timestomp.exe
- Énoncé du TP - Timestomp : altération de l'horodatage de la $MFT
- Conclusion du cours