Programme - Investigation numérique Windows

Investigation numérique Windows	
Durée	3 jours
Public	Administrateur, analyste SOC, ingénieur sécurité
Pré-requis	Connaissance sur l'OS Windows, TCP/IP, Linux
Objectifs	Acquérir les compétences et la méthodologie pour une investigation numérique sur le système d'exploitation Windows
Plan de cours	Jour 1 matin ***Section 1 - Etat de l'art de l'investigation numérique*** • **Introduction à l'investigation numérique** • **Vocabulaire** • **Les différentes disciplines** • **Indicateur de compromission** • **Méthodologie d'investigation** • **ATT&CK et Arbres d'attaque** **Jour 1 après-midi** ***Section 2 - Les fondamentaux Windows et Collecte des données*** • **Fondamentaux Windows**

- **Structure des répertoires**
- **Séquence de boot**
- **Bases de Registres**
- **Logs et événements**
- **Services**
- **Volume Shadow Copy Service**
- **Généralités sur les disques durs**
- **Fondamentaux NTFS**
- **Analyse live**
- **Analyse offline : imaging**
- **Analyse offline : collecte**
- **Les outils d'analyse**

Jour 2 matin
Section 3 - Artefacts

- **Différents artefacts internet**
- **Pièces jointes**
- **Open/Save MRU**
- **Flux ADS Zone.Identifier**
- **Téléchargements**
- **Historique Skype**
- **Navigateurs internet**
- **Historique**
- **Cache**
- **Sessions restaurées**
- **Cookies**
- **Différents artefacts exécution**
- **UserAssist**
- **Timeline Windows 10**
- **RecentApps**
- **Shimcache**
- **Jumplist**
- **Amcache.hve**
- **BAM/DAM**
- **Last-Visited MRU**
- **Prefetch**

Jour 2 après-midi

- **Différents artefacts fichiers/dossiers**
- **Shellbags**
- **Fichiers récents**

- **Raccourcis (LNK)**
- **Documents Office**
- **IE/Edge Files**
- **Différents artefacts réseau**
- **Termes recherchés sur navigateur**
- **Cookie**
- **Historique**
- **SRUM (ressource usage monitor)**
- **Log wifi**
- **Différents artefacts comptes utilisateur**
- **Dernières connexions**
- **Changement de mot de passe**
- **Echec/Réussite d'authentification**
- **Évènement de service (démarrage)**
- **Evènement d'authentification**
- **Type d'authentification**
- **Utilisation du RDP**
- **Différents artefacts USB**
- **Nomination des volumes**
- **Evénement PnP (Plug & Play)**
- **Numéros de série**
- **Différents artefacts fichiers supprimés**
- **tools**
- **Récupération de la corbeille**
- **Thumbcache**
- **Thumb.db**
- **WordWheelQuery**
- **Spécificités Active Directory**
- **TP 3 / Première investigation**
- **TP 4 / Deuxième investigation**

Jour 3 matin
Section 4 - Analyse mémoire et Anti Forensic

- **Acquisition**
- **Volatility**
- **TP 5 / Investigation mémoire**
- **Principes d'Anti Forensic**
- **Techniques d'Anti Forensic**

Jour 3 après-midi

- **Tools pour Anti Forensic**

	• **TP6 / Anti Forensic** ❏