Sécurité défensive

Investigation numérique Windows (Computer Forensics)

3 jours (21h00) | ★★★★☆ 4/5 | SEC-INFW | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel

Contenu mis à jour le 18/10/2024. Document téléchargé le 08/12/2024.

Objectifs de formation

A l'issue de cette formation, vous serez capable de :

- Identifier les principes fondamentaux du Forensic sous Windows
- Décrire les méthodes et outils de collecte de données
- Analyser un système de fichiers
- Analyser la mémoire et les artefacts du système
- Rédiger un rapport et présenter des résultats.

Modalités, méthodes et moyens pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2i, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

* *nous consulter pour la faisabilité en distanciel*

** *ratio variable selon le cours suivi*

Prérequis

Avoir de bonnes connaissances sur le hacking, la sécurité et Windows.

Public concerné

Administrateurs systèmes et réseau, analystes SOC, RSSI, pentesteurs et/ou auditeurs.

Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

Programme

Jour 1

Introduction et principes fondamentaux

- Définition et importance de l'informatique légale
- Principes et méthodologies de base
- Les différents types de criminalistique informatique
- Légalité et conformité de la démarche
- Considérations éthiques dans les investigations
- Les méthodes de collecte de preuves numériques
- L'identification et la préservation des preuves
- L'importance de la timeline
- Le laboratoire d'investigation
- Minimiser les interférences avec le sujet
- Automatiser les processus

Déterminer s'il s'agit d'un incident

- Méthodologie et points d'importance
- Présentation du framework ATT&CK du MITRE et points d'entrée des cyberattaques
- Les signes de compromission (corrélation ATT&CK)

Environnement Windows

- Les enjeux de Windows dans le domaine de l'informatique légale
- Les éléments de base d'un environnement Windows dans le contexte du Computer Forensics
- Les outils populaires
  - FTK
  - EnCase
  - Autopsy
  - Sleuth Kit
  - X-Ways Forensics
  - Volatility...

Exemples de travaux pratiques (à titre indicatif)

- *Installation et configuration d'un environnement d'investigation*
- *Déploiement d'outils, dont Autopsy, et du Sleuth Kit dans l'environnement d'investigation*

La collecte de données

- La création d'images disques

    - FTK Imager
    - EnCase
    - ProDiscover Forensic
    - OSForensics...
- La capture de la mémoire vive
    - DumpIt
    - WinPmem
    - Volatility
    - Belkasoft RAM Capturer
    - Memoryze
    - FTK Imager...
- Créer une image depuis une machine virtuelle
- L'obfuscation sur un système Windows
- Les élévations de privilèges
- L'anti-Forensic et le Timestomping
- La gestion et le stockage sécurisé des données
    - Stratégies de stockage sécurisé
    - Le rôle du hash de l'image
- Bloquer les écritures logicielles et matérielles
- La documentation des processus de collecte

Exemples de travaux pratiques (à titre indicatif)

- *Création d'un clone de disque dur à froid*
- *Création d'un clone de disque dur et dump mémoire à chaud*
- *Documenter les actions réalisées*

Jour 2

L'analyse de la mémoire morte

- L'analyse des partitions
- La structure des systèmes de fichiers (FAT32, NTFS...)
- Les VSS (Volume Shadow Copy Service)
- La recherche des métadonnées
- Les différents artefacts d'exécution
    - Prefetch
    - Last-visited MRU
    - UserAssist
    - ShimCache
    - RecentApps
    - Jumplist
    - Timeline Windows 10
    - Amcache.hve
    - BAM / DAM
- Les différents artefacts d'activité des fichiers et dossiers
    - Shellbags
    - Fichiers récents
    - Raccourcis (LNK)
    - Récupération de la corbeille
    - Thumbcache
    - Thumb.db
    - WordWheelQuery
    - Documents Office
    - IE / Edge files
- Les différents artefacts des comptes utilisateurs

  - Dernières connexions
  - Changement de mot de passe
  - Echec / réussite d'authentification
  - Evènement de service (démarrage)
  - Evènement d'authentification
  - Type d'authentification
  - Utilisation du RDP (Remote Desktop Protocol)
- Les différents artefacts réseau
  - Le cache des connexions TCP/IP
  - Les logs des connexions aux réseaux Ethernet et Wi-Fi
  - Le cache ARP
  - Le cache DNS
  - Les tables de routage
  - Les connexions VPN
  - Flux ADS Zone. Identifier
  - SRUM (System Resource Usage Monitor)
  - Navigateurs Internet (Open / Save MRU, téléchargements, cookies, historique, cache, sessions restaurées)
- Les différents artefacts USB
  - Nomination des volumes
  - Evènement PnP (Plug et Play)
  - Numéros de série
- Les techniques de récupération de données
  - Récupération de fichiers supprimés
  - Les méthodes utilisées par le Sleuth Kit et Autopsy
- Trouver et examiner les "File Slacks"
- Extraire, stocker et analyser les hashes des fichiers
- Utiliser le Carving
- Les malwares
  - Retrouver une signature
  - Utiliser les strings
- Le rapport d'analyse

Exemples de travaux pratiques (à titre indicatif)

- *Analyse d'un système de fichiers post-mortem*
- *Recherche de données cachées sur une image disque*
- *Recherche d'outils malveillants présents sur le système*
- *Rédaction succincte d'un rapport d'analyse des éléments présents*

Jour 3

L'analyse de la mémoire vive

- La structure de la mémoire vive sous Windows
- Les outils pour l'analyse de la mémoire
- L'identification des processus actifs
- Tracer les appels système
- Tracer les appels de librairies
- L'analyse des structures de données
- L'analyse des modules chargés
- L'étude des connexions réseau
- L'extraction des artefacts
- La recherche de malwares

Exemples de travaux pratiques (à titre indicatif)

- *Analyse d'un dump mémoire*
- *Recherche des processus présents*
- *Recherche d'outils malveillants*

- *Extraction d'artefacts*
- *Mise en évidence des éléments d'intérêt*

La corrélation

- Création de la timeline
- Corrélation des éléments entre les différentes analyses

Exemples de travaux pratiques (à titre indicatif)

- *Création d'une timeline sur la base des éléments collectés dans les travaux pratiques précédents*
- *Détermination du scénario d'attaque de l'ensemble des éléments évoqués*

La rédaction du rapport d'analyse

- Les éléments du rapport
- Le formalisme du rapport
- La diffusion et le stockage du rapport

Le contenu de ce programme peut faire l'objet d'adaptation selon les niveaux, prérequis et besoins des apprenants.

Modalités d’évaluation des acquis

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation

Accessibilité de la formation

Le groupe M2i s'engage pour faciliter l'accessibilité de ses formations. Toutes nos formations sont accessibles aux personnes en situation de handicap : les détails de l'accueil des personnes sont consultables sur la page Accueil PSH.

Modalités et délais d’accès à la formation

Les formations M2i sont disponibles selon les modalités proposées sur la page programme.
Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation.
Dans le cas d'une formation financée par le CPF, ce délai est porté à 11 jours ouvrés.