Sécurité défensive

Investigation numérique (Computer Forensics)

5 jours (35h00) | ★★★★½ 4,6/5 | SEC-INVFOR | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel

Contenu mis à jour le 18/10/2024. Document téléchargé le 23/01/2025.

Objectifs de formation

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

- Identifier les principes fondamentaux du Forensic des systèmes et des réseaux
- Mettre en pratique les méthodes et outils de collecte de données sous Windows et Linux
- Analyser un système de fichiers Windows et Linux
- Analyser la mémoire et les artefacts du système sous Windows et Linux
- Utiliser les techniques d'acquisition, d'analyse et d'interprétation des données réseau
- Utiliser les outils Windows ou Linux pour la collecte et l'analyse des données réseau
- Appliquer les meilleures pratiques pour sécuriser et documenter les investigations numériques
- 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, les systèmes Windows et Linux, le modèle OSI et les protocoles TCP/IP.

Public concerné

Administrateurs systèmes et réseau, analystes SOC, RSSI, pentesteurs 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
- 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
- Créer une image depuis une machine virtuelle

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 (Forensic ToolKit)
- EnCase
- Autopsy
- The 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 The Sleuth Kit, dans l'environnement d'investigation*

La collecte de données en environnement Windows

- La création d'images disques :
  - FTK Imager
  - EnCase
  - ProDiscover Forensics
  - OSForensics...
- La capture de la mémoire vive :
  - DumpIt
  - WinPMem
  - Volatility
  - Belkasoft RAM Capturer
  - Memoryze
  - FTK Imager...

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*

L'analyse de la mémoire morte en environnement Windows

- L'analyse des partitions
- La structure des systèmes de fichiers (FAT32, NTFS...)
- Les VSS (Volume Shadow Copy Service)
- La recherche des métadonnées

Jour 2

L'analyse de la mémoire morte en environnement Windows - Suite

- Les différents artefacts :
  - D'exécution
  - D'activité des fichiers et dossiers
  - Des comptes utilisateurs
  - Réseau
  - USB
- Les techniques de récupération de données
  - Récupération de fichiers supprimés
  - Les méthodes utilisées par The 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*

L'analyse de la mémoire vive en environnement Windows

- 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*

Jour 3

Environnement Linux

- Les enjeux de Linux dans le domaine de l'informatique légale
- Les éléments de base d'un environnement Linux dans le contexte du Computer Forensics
- Les distributions et les outils populaires
  - Kali Linux, CAINE, DEFT Linux, SIFT, Tsurugi Linux
  - Autopsy, The Sleuth Kit, FTK Imager, dd...

Exemples de travaux pratiques (à titre indicatif)

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

La collecte de données en environnement Linux

- La création d'images disques
  - dd, dcfldd, FTK Imager, Guymager...
- La capture de la mémoire vive
  - LiME, Volatility, PMem, Memdump, FTK Imager...

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*

L'analyse de la mémoire morte en environnement Linux

- L'analyse des partitions
- La structure des systèmes de fichiers (ext3, ext4...)
- Les superblocs
- Les caractéristiques du système de fichiers étendu
- La recherche des métadonnées

- Le GUID
- La recherche des modifications
- L'examen :
  - Des fichiers "history"
  - Des fichiers de logs
  - Des fichiers temporaires
  - Des configurations réseau
- Les techniques de récupération de données
  - Récupération de fichiers supprimés
  - Les méthodes utilisées par The 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 4

L'analyse de la mémoire vive en environnement Linux

- La structure de la mémoire vive sous Linux
- 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*

Les équipements réseaux

- Les enjeux du réseau dans le domaine de l'informatique légale
- Les éléments de base d'un environnement réseau dans le contexte du Computer Forensics
- Les équipements et leurs rôles
  - Switches, routeurs, firewalls, firewalls NG, IPS, IDS, Syslogs, SIEM...
- Les distributions et les outils populaires
  - Kali, Parrot Security OS, BlackArch Linux, CAINE, NST, Tails...
  - Wireshark, Nmap, TCPdump, WINdump, netcat, snort, ettercap, Zeek...

Exemples de travaux pratiques (à titre indicatif)

- *Installation et configuration d'un environnement d'investigation*
- *Déploiement d'outils, dont Nmap et Wireshark, sur un environnement en mode pont transparent*

La collecte de données

- Les types de données réseau
- Le positionnement de la sonde de capture
- Les méthodes d'acquisition (passives et actives)
- Les outils d'acquisition
- La capture de trafic :
  - Sur les appliances
  - En environnement virtuel avec NFV

Exemples de travaux pratiques (à titre indicatif)

- *Capture d'un trafic réseau avec Windows ou Linux*
- *Analyse d'un trafic obfusqué*
- *Documenter les actions réalisées*

Jour 5

L'analyse des paquets

- Structure des paquets réseau
- Identification des protocoles et services
- Types de menaces (DoS, DDoS, Man-in-the-Middle...)
- Analyse des sessions TCP
- Les protocoles nécessitant l'attention de l'investigateur
- Techniques de détection et d'analyse des malwares

Exemples de travaux pratiques (à titre indicatif)

- *Utilisation d'un analyseur de paquets pour afficher, filtrer, isoler et analyser un trafic spécifique*
- *Détermination de l'usage réel d'un flux réseau*
- *Identification de trafics illégitimes*
- *Documentation des actions réalisées*

Exploitation de sondes IPS et IDS

- Le rôle des IPS et des IDS
- Le positionnement des sondes
- La gestion des paramètres principaux
- La gestion des règles

Exemples de travaux pratiques (à titre indicatif)

- *Installation d'un IPS ou d'un IDS sous Windows ou Linux*
- *Paramétrage de la sonde et de la remontée d'alerte*
- *Création de règles personnalisées correspondant à l'environnement de formation*
- *Détection d'un trafic illégitime en temps réel*

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*

Examen M2i (en option)

- Prévoir l'achat de l'examen en supplément
- L'examen (en français) sera passé le dernier jour, à l'issue de la formation et s'effectuera en ligne

- Il s'agit d'un QCM dont la durée moyenne est d'1h30 et dont le score obtenu attestera d'un niveau de compétence
- L'examen n'est pas éligible au CPF, mais permettra néanmoins de valider vos acquis

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 et/ou un examen M2i

Les + de la formation

Un examen M2i permettant de valider vos acquis à l'issue de la formation est disponible sur demande (coût : 120€).

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.