



Sécurité défensive

Investigation numérique Linux (Computer Forensics)

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

Formations Informatique › Cybersécurité › Sécurité défensive

Contenu mis à jour le 13/10/2023. Document téléchargé le 29/05/2024.

Objectifs de formation

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

- Réaliser des analyses Forensics sur Linux.

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 Linux.

Public concerné

Administrateurs réseaux et systèmes, 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

- Définition du Forensic
- Les types de Forensics
- Linux et le Forensic
- Principes généraux
- Phases d'investigation
- Les hauts niveaux de process

Exemple de travaux pratiques (à titre indicatif)

- *Réaliser un Toolkit*

Déterminer s'il s'agit d'un incident

- Méthodologie
- Minimiser les interférences avec le sujet
- Automatiser les process

Exemple de travaux pratiques (à titre indicatif)

- *Collecter les données volatiles*

Analyses

- Rechercher les métadonnées
- Reconstituer une chronologie
- Examiner l'history
- Rechercher les logs
- Collecter les hashes

Exemple de travaux pratiques (à titre indicatif)

- *Dumper la rame*

Jour 2

Création d'images

- Les formats d'images
- Utiliser DD
- Utiliser DCFLDD
- Bloquer les écritures logicielles et matérielles

- Créer une image depuis une VM

Exemple de travaux pratiques (à titre indicatif)

- Créer une image depuis un disque dur

Analyse des images

- Les partitions
- Le GUID
- Automatiser le montage
- Rechercher toutes les modifications
- Importer les informations dans une base de données
- Examiner les logs

Exemple de travaux pratiques (à titre indicatif)

- Créer une chronologie

Analyse du système de fichiers étendu

- Les fondamentaux
- Les superblocs
- Caractéristiques du système de fichiers étendu
- Automatisation de l'analyse
- Retrouver les incohérences
- Inodes journalisation

Analyse de la mémoire Volatility

- Prise en main de Volatility
- Cartographier les process
- Retrouver les informations réseau
- Retrouver les informations du système de fichiers
- Commandes avancées

Exemple de travaux pratiques (à titre indicatif)

- Analyse d'un dump mémoire

Jour 3

Réagir aux attaques avancées

- Etat des attaques PFE
- Analyse mémoire avancée
- Analyse avancée du système de fichiers
- Utiliser MySQL
- Autres recherches

Exemple de travaux pratiques (à titre indicatif)

- Analyse avancée du système de fichiers

Malwares

- Les commandes
- Retrouver une signature
- Utiliser les strings
- Utiliser nm
- Utiliser ldd
- Utiliser objdump
- Tracer les appels système
- Tracer les appels de bibliothèques

- Utiliser GNU Debugger
- Obfuscation

Exemple de travaux pratiques (à titre indicatif)

- Retrouver une signature sur un malware

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. Les détails de l'accueil des personnes en situation de handicap sont consultables sur la page Accueil et Handicap.

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.