Développez vos talents
Certifiez vos compétences

Sécurité défensive

Investigation numérique Linux (Computer Forensics)

3 jours (21h00) | ★★★★½ 4,4/5 | SEC-INFL | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel [1]

Formations Informatique › Cybersécurité › Sécurité défensive

À l'issue de ce stage vous serez capable de :

- Acquérir les connaissances pour réaliser les analyses Forensics sur Linux.

Niveau requis

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.

(1) Modalité et moyens pédagogique :

Formation délivrée en présentiel ou distanciel * (e-learning, classe virtuelle, présentiel à distance). Le formateur alterne entre méthodes ** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification.

Les moyens pédagogiques mis en oeuvre (variables suivant les formations) sont : ordinateurs Mac ou PC (sauf pour les 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.

* Nous consulter pour la faisabilité en distanciel. ** Ratio variable selon le cours suivi.

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*

Analyses 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 librairies
- Utiliser GNU Debugger
- Obfuscation

Exemple de travaux pratiques (à titre indicatif)

- *Retrouver une signature sur un malware*

Modalités d'évaluation des acquis

L'évaluation des acquis se fait :

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation ou une certification (M2i ou éditeur)