Développez vos talents
Certifiez vos compétences

Sécurité défensive

Investigation numérique Web (Web Forensics)

2 jours (14h00) | ★★★★½ 4,6/5 | SEC-INFWEB | 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 :

- Analyser de façon méthodique un serveur Web compromis.

Niveau requis

Avoir des connaissances en programmation Web, système, Bash et Linux.

Public concerné

Pentesters et développeurs.

Partenaire / éditeur

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

- Chiffres
- Rappels
- Panorama des attaques Web (top 10 OWASP)
- Le monde de l'investigation
- Le contexte spécifique au Web

De la méthodologie à la pratique

- La méthode / approche
- Temporalité (MAC times et timezones)
- Créer un arbre d'attaque
- Capturer un environnement Web

Exemple de travaux pratiques (à titre indicatif)

- *Première intervention*

Principaux artefacts

- Les process
- Logs
- Inspection de la base de données
- Inspection du système de fichiers
- Analyse statique
- Désobfuscation de charge

Exemple de travaux pratiques (à titre indicatif)

- *Collecte et examen d'artefacts*

Regex

- Principes
- Création d'outils
- Parser des logs

Exemple de travaux pratiques (à titre indicatif)

- *Analyse de logs*

Jour 2

Exemples de travaux pratiques (à titre indicatif) : scénario d'attaques

- *Brute force SSH*
- *WebShell*
- *File inclusion*
- *XSS / Frames*
- *Injection SQL*

Rédaction d'un rapport

- Eléments clés
- Méthodologie
- Réponse à incident

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)