Analyse Forensic et réponse à incidents de sécurité

★★★★★

PL-54 **4 Jours (28 Heures)**

Description

Ce stage avancé vous montrera les techniques indispensables pour réaliser une analyse post-mortem (aussi appelée inforensic) d'incidents de sécurité informatiques. Suite à des simulations d'attaques, vous apprendrez à collecter et préserver les preuves, les analyser et améliorer la sécurité du SI après l'intrusion.

À qui s'adresse cette formation ?

Pour qui

Ingénieur/administrateur systèmes et réseaux, responsable de la sécurité.

Prérequis

Aucun

Les objectifs de la formation

- Maîtriser les bons réflexes en cas d'intrusion sur une machine
- Collecter et préserver l'intégrité des preuves électroniques
- Analyser l'intrusion a posteriori
- Améliorer sa sécurité après une intrusion

Programme de la formation

Analyse forensic (ou inforensic) des systèmes

- Informatique judiciaire.
- Types de crimes informatiques.
- Rôle de l'enquêteur informatique.

Cybercriminalité moderne

- Types de criminalité.
- Cadre de gestion d'un incident de sécurité, CERT.
- Analyser et comprendre les attaques réseaux.
- Détection réseau d'intrusions.
- Outils de protection, législation française.
- Travaux pratiques Analyser des logs réseaux d'un DDoS Volumétrique, ARP.
- Mise en place de SNORT.

Analyse forensic d'un système d'exploitation Windows

- Acquisition, analyse et réponse.
- Compréhension des processus de démarrage.
- Collecter les données volatiles et non volatiles.
- Fonctionnement du système de mot de passe, du registre Windows.
- Analyse des données contenues dans la mémoire vive, des fichiers Windows.
- Analyse du cache, cookie et historique de navigation, historique des événements.
- Travaux pratiques Injection d'un utilisateur.
- Casser le mot de passe.
- Collecter, analyser les données de la mémoire vive.
- Référencer, faire le hash de tous les fichiers.
- Explorer les données du navigateur, du registre.

Analyse de logs

- Visualiser, trier, chercher dans les traces.
- Splunk pour comprendre les attaques.
- Travaux pratiques Installer, configurer Splunk.
- Analyser des logs Web d'un Brute-Force sur Formulaire, mise en place de contre-mesure.

Collecte des informations

- Hétérogénéité des sources.
- Qu'est-ce qu'un événement de sécurité ? Security Event Information Management (SIEM), événements collectés du SI.
- Journaux système des équipements (firewalls, routeurs, serveurs, bases de données).
- Travaux pratiques Géolocalisation d'adresses.
- Analyse de l'historique des utilisateurs Web (cookie, données envoyées POST).
- Analyser des logs Web d'une Injection SQL et mise en place de contre-mesure.

Preuve numérique

- Définition, rôle, types et règles de classement.
- Evaluer et sécuriser les éléments électroniques d'une scène de crime.
- Collecter et préserver l'intégrité des preuves électroniques.
- Travaux pratiques Dupliquer les données bit à bit, vérifier l'intégrité.
- Récupérer les fichiers supprimés et/ou cachés.
- Analyse des données numériques.