Syllabus

Criminalistique Windows

CYBERIUM ARENA

— SIMULATOR —

En partenariat avec : SERTI

La description

Windows Forensics est une compétence essentielle dans le monde de la cybersécurité. Ce cours couvre un large éventail d'aspects du processus d'enquête légale exécuté sur le système d'exploitation Windows. Les participants apprendront comment fonctionnent différents composants informatiques et comment enquêter après un cyber-incident. La formation se concentrera sur le développement des capacités pratiques des équipes criminalistiques ou des praticiens individuels.

Le cours aide à préparer les examens de certification CHFI (CE | Conseil) et GCIH(SANS).

Public cible

Ce cours s'adresse aux participants ayant des connaissances de base qui souhaitent comprendre les cybers-enquêtes.

Objectifs

- Comprendre la structure des fichiers Windows
- Accès aux fichiers cachés sur le système
- Extraction d'informations sensibles
- Maîtriser les étapes de réponse aux incidents

Module 1: Matériel informatique

Le module couvrira différents composants du matériel informatique. Les étudiants apprendront les principaux composants des disques de stockage, la structure du système d'exploitation Windows et installeront des stations de criminalistique virtuelles.

Lecteurs et disques
- Représentation des données
- Volumes et partitions
- Partitionnement de disque et outil de gestion de disque
- Caractéristiques du disque SSD (Solid State Drive)

Comprendre la structure du système d'exploitation Windows
- Structure NTFS
- Table de fichier maitre
- Fichiers système Windows

Structure des données et des fichiers
- Éditeurs hexadécimaux
- Structure des fichiers

Module 2: Fondamentaux de la criminalistique

Dans ce module, les étudiants apprendront les composants internes du système d'exploitation Windows et le processus d'enquête forensique.

Comprendre les hachages et les codages
- L'utilisation du hachage pour la criminalistique
- Encodages de base

Artefacts Windows
- Fichiers de démarrage
- Liste des sauts
- Cache de miniatures
- Cliché instantané
- Répertoires de prélecture et temporaire
- Applications récentes
- Ruches du registre
- Métadonnées intégrées

Module 3: Collecte de preuves

Les étudiants maîtriseront les techniques de collecte de preuves, d'accès et de récupération d'informations volatiles et non volatiles au cours de ce module.

Sculpture de données forensiques
- Sculpture manuelle
- Outils automatiques

Collecte d'informations
- Observateur d'événements
- Détection des fichiers cachés
- Collecte d'informations sur le réseau
- Sysinternals
- Extraction des informations d'identification

Module 4: Analyse des résultats d'investigation

Dans ce module, les étudiants comprendront comment découvrir des informations cachées, détecter les fichiers falsifiés, travailler avec la mémoire et analyser le Ram.

Acquisition de données des lecteurs
- Créer une image
- Analyse des fichiers de prélecture

Travailler avec la mémoire volatile
- Extraire des données de la RAM
- Identification des connexions réseau
- Décharger les processus de la mémoire

Analyse du registre
- Affichage des vidages de registre
- Utilisation du fichier Dat
- Constatations forensiques dans le registre

Techniques anti-forensiques
- Effacement des disques
- Suppression d'artefact