Microtel
Training institute

COMPUTER HACKING FORENSIC INVESTIGATOR

CURSUS:
EC-COUNCIL

CODE DE LA FORMATION:
EC-SC-CHFI

VERSION:
8.0

DURÉE:
5 JOURS

Le cours CHFI donnera aux participants les qualifications nécessaires pour identifier les traces laissées lors de l'intrusion d'un système informatique par un tiers et pour collecter correctement les preuves nécessaires à des poursuites judiciaires.
L'usage de nombreux outils incontournables sera enseigné durant cette formation : software, hardware et techniques spécifiques.
Le besoin pour l'entreprise de devenir plus efficace et intégrée avec ses partenaires, ainsi que le développement de l'informatique personnelle ont donné naissance à un nouveau type de criminel, le « cyber criminel » Il n'est plus question de savoir si votre entreprise va être un jour attaquée, mais plutôt quand.
Ce cours est adapté si vous ou votre entreprise avez besoin de connaissances pour identifier, traquer et poursuivre judiciairement des cybers criminels.

PUBLIC:
Cette formation est destinée à la police, personnels militaires et de la défense, professionnels de la sécurité Ebusiness, administrateurs systèmes, professions juridiques, Banque, assurance et autres professionnels, organismes gouvernementaux, responsables informatiques.

OBJECTIFS:
- Donner aux participants les qualifications nécessaires pour identifier les traces laissées lors de l'intrusion d'un système informatique par un tiers et pour collecter correctement les preuves nécessaires à des poursuites judiciaires
- Préparer à l'examen CHFI EC0 312-49 à l'issue du cours

CONTENU:
- Investigation légale dans le monde d'aujourd'hui
- lois sur le Hacking et la légalité dans l'informatique
- Procédés d'investigation informatique
- Procédure « First Responder »
- CSIRT
- Laboratoire d'investigation légale
- Comprendre les systèmes de fichiers et les disques durs
- Comprendre les appareils multimédia digitaux
- Processus de lancement Windows, Linux et Mac
- Investigation légale dans IWindows
- Investigation légale dans Linux
- Acquisition de données et duplication
- Outils d'investigation légale
- Investigations légales utilisant Encase
- Retrouver des fichiers et des partitions supprimés

- Investigation légale dans les fichiers d'images
- Stéganographie
- Application de crackage de mots de passe
- Investigation légales dans les réseaux et utiliser les journaux de logs à des fins d'investigation
- Enquêter sur le trafic réseau
- Enquêter sur les attaques Wireless
- Enquêter sur des attaques internet
- Investigation légale de routeurs
- Enquêter sur les attaques par Déni de Service
- Enquêter sur les cybercrimes
- Suivre les emails et enquêter sur les délits par email
- Enquêter sur l'espionnage industriel
- Enquêter sur les atteintes portées aux marques déposées et copyright
- Enquêter sur les incidents de harcèlement sexuel
- Enquêter sur la pornographie enfantine
- Investigation légale de PDA
- Investigation légale d'Ipod
- Investigation légale de Blackberry
- Rapports d'investigation
- Devenir un témoin-Expert

CERTIFICATION:

L'examen de CHFI *312-49* sera planifié le dernier jour de la formation. Après avoir suivi le stage vous passerez un QCM en ligne de 150 questions (en Anglais) pendant 4h.