Sécurité : Préparation à la certification CHFI, Computer Hacking Forensic Investigator v8

Formation Informatique / Réseaux et Sécurité / Sécurité

OBJECTIFS

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.
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.
Préparation à l'examen CHFI EC0 312-49 à l'issue du cours. **L'examen de CHFI 312-49 sera planifié le dernier jour de la formation. Les étudiants doivent passer l'examen en ligne de Prometric pour recevoir la certification de CHFI.**

YA-CONSULTATION
(225) 01 52 22 63 12

PUBLIC

Ce cours est destiné à la police, personnels militaires et de la défense, professionnels de la sécurité E-business, administrateurs systèmes, professions juridiques, Banque, assurance et autres professionnels, organismes gouvernementaux, responsables informatiques.

PRE-REQUIS

Il est fortement recommandé d'avoir validé le CEH (certified ethical hacker) avant de suivre le cours CHFI.

PROGRAMME

Jour n°1
Module 1 : l'investigation légale dans le monde d'aujourd'hui
Module 2 : lois sur le Hacking et la légalité dans l'informatique
Module 3 : Procédés d'investigation informatique
Module 4 : Procédure « First Responder »
Module 5 : CSIRT
Module 6 : Laboratoire d'investigation légale
Module 7 : Comprendre les systèmes de fichiers et les disques durs
Module 8 : Comprendre les appareils multimédia digitaux

Jour n°2
Module 9 : Processus de lancement Windows, Linux et Mac
Module 10 : Investigation légale dans IWindows
Module 11 : Investigation légale dans Linux
Module 12 : Acquisition de données et duplication
Module 13 : Outils d'investigation légale
Module 14 : Investigations légales utilisant Encase

Jour n°3
Module 15 : Retrouver des fichiers et des partitions supprimés
Module 16 : Investigation légale dans les fichiers d'images
Module 17 : Stéganographie
Module 18 : Application de crackage de mots de passe
Module 19 : Investigation légales dans les réseaux et utiliser les journaux de logs à des fins d'investigation
Module 20 : Enquêter sur le trafic réseau
Module 21 : Enquêter sur les attaques Wireless

Jour n°4
Module 22 : Enquêter sur des attaques internet
Module 23 : Investigation légale de routeurs
Module 24 : Enquêter sur les attaques par Déni de Service
Module 25 : Enquêter sur les cybercrimes
Module 26 : Suivre les emails et enquêter sur les délits par email
Module 27 : Enquêter sur l'espionnage industriel
Module 28 : Enquêter sur les atteintes portées aux marques déposées et copyright

Jour n°5
Module 29 : Enquêter sur les incidents de harcèlement sexuel

Sécurité : Préparation à la certification CHFI, Computer Hacking Forensic Investigator v8

Formation Informatique / Réseaux et Sécurité / Sécurité

Module 30 : Enquêter sur la pornographie enfantine
Module 31 : Investigation légale de PDA
Module 32 : Investigation légale d'Ipod
Module 33 : Investigation légale de Blackberry
Module 34 : Rapports d'investigation
Module 35 : Devenir un témoin-Expert

YA-CONSULTING
(225) 01 52 22 63 12