Computer Hacking Forensic Investigator (CHFI)

Description

En quoi consiste la formation Computer Hacking Forensic Investigator (CHFI) ?

La formation Computer Hacking Forensic Investigator (CHFI) est un programme complet pour les professionnels souhaitant maîtriser l'art du forensique numérique. À une époque où les cyberattaques se multiplient, il est essentiel de savoir collecter et analyser les preuves numériques. Ce cours vous permet d'acquérir des compétences pratiques pour enquêter sur des incidents de sécurité informatique, qu'ils se produisent sur des ordinateurs, des réseaux, ou même des environnements cloud.

Pourquoi suivre cette formation ?

En suivant ce programme, vous apprendrez à identifier les traces laissées par les pirates, à sécuriser et dupliquer les données sensibles, et à défendre contre les techniques anti-forensiques. Cette certification CHFI vous donne également les compétences pour analyser des attaques complexes sur divers systèmes, y compris Windows, Linux, et les dispositifs mobiles. Si vous travaillez dans la sécurité informatique ou souhaitez évoluer dans ce domaine, cette formation est incontournable pour acquérir des compétences avancées en investigation numérique.

Contenu du cours
Module 1 : Computer Forensics in Today's World

- Introduction aux enjeux actuels du forensique numérique
- Rôles et responsabilités dans une enquête forensique

Module 2 : Computer Forensics Investigation Process

- Étapes clés de l'investigation forensique
- Collecte et préservation des preuves numériques

Module 3 : Understanding Hard Disks and File Systems

- Fonctionnement des disques durs
- Analyse des systèmes de fichiers (FAT, NTFS, ext)

Module 4 : Data Acquisition and Duplication

- Méthodes d'acquisition des données
- Techniques de duplication sécurisée des données

Module 5 : Defending Anti-Forensics Techniques

- Identification des techniques anti-forensiques
- Stratégies de défense contre ces techniques

Module 6 : Windows Forensics

- Collecte et analyse de preuves sur Windows
- Utilisation des outils forensiques pour Windows

Module 7 : Linux and Mac Forensics

- Analyse forensique sur Linux et Mac
- Outils et techniques pour ces systèmes

Module 8 : Network Forensics

- Enquête sur les attaques réseau
- Collecte et analyse de données réseau

Module 9 : Malware Forensics

- Analyse de logiciels malveillants
- Étude des traces laissées par les malwares

Module 10 : Investigating Web Attacks

- Enquête sur les attaques web
- Identification des vulnérabilités exploitables

Module 11 : Dark Web Forensics

- Analyse des activités sur le Dark Web
- Outils et techniques pour enquêter

Module 12 : Cloud Forensics

- Enquête forensique dans les environnements cloud
- Collecte de preuves sur les plateformes cloud

Module 13 : Email and Social Media Forensics

- Analyse des preuves issues des emails
- Investigation sur les réseaux sociaux

Module 14 : Mobile Forensics

- Collecte de preuves sur les dispositifs mobiles
- Outils et techniques pour l’investigation mobile

Module 15 : IoT Forensics

- Enquête sur les appareils IoT
- Challenges et opportunités du forensique IoT

Documentation

- Support de cours numérique inclus

Examen

- Ce cours prépare à la certification Computer Hacking Forensic Investigator (CHFI).
- Pour obtenir la certification Computer Hacking Forensic Investigator (CHFI), les candidats doivent réussir l'examen : 312-49.
- Nombre de questions : 150
- Durée : 4 heures
- Si vous souhaitez passer cet examen, veuillez contacter notre secrétariat qui vous informera du coût des examens et prendra en charge toutes les démarches administratives nécessaires pour vous.

Profils des participants

- Professionnels de la cybersécurité
- Administrateurs systèmes et réseaux
- Analystes en sécurité informatique
- Experts en gestion des incidents de sécurité
- Consultants en forensique numérique

Connaissances Préalables

- Connaissances de base en sécurité informatique
- Compréhension des systèmes d'exploitation (Windows, Linux, Mac)
- Notions de réseaux et d'infrastructures IT
- Expérience en gestion d'incidents de sécurité

Objectifs

- Comprendre le processus d'investigation forensique
- Analyser des disques durs et des systèmes de fichiers
- Acquérir et dupliquer des données sensibles
- Défendre contre les techniques anti-forensiques
- Enquêter sur des attaques réseau et Web
- Analyser les preuves sur les systèmes Windows, Linux et Mac

Description
Formation Computer Hacking Forensic Investigator (CHFI)
Niveau
Intermédiaire
Prix de l'inscription en Présentiel (CHF)
5900
Prix de l'inscription en Virtuel (CHF)
5650
Durée (Nombre de Jours)
5
Reference
CHFI