Certified Hacking Forensic Investigator (CHFI)

CODICE	**DT0102**
DURATA	**5 gg**
PREZZO	**3.500,00 €**
EXAM	

DESCRIZIONE

Le tecnologie digitali stanno cambiando il mondo professionale e di conseguenza le organizzazioni si devono adattare rapidamente alle nuove tecnologie come il cloud, il mobile, i big data o l'IoT. In questo scenario l'informatica "forense" sta ormai diventando una necessità.

Il corso Certified Hacking Forensic Investigator (CHFI) aggiornato, alla versione 11, fornisce ai suoi partecipanti una solida padronanza della digital forensics, presentando un approccio dettagliato e metodologico alla digital forensics e all'analisi delle prove che ruota anche intorno al Dark Web, IoT e Cloud Forensics. Gli strumenti e le tecniche coperte in questo programma prepareranno lo studente a condurre indagini digitali utilizzando tecnologie forensi digitali all'avanguardia.

Ciò include la definizione del processo forense, delle procedure di laboratorio e di gestione delle prove, nonché le procedure di indagine necessarie per convalidare/triage degli incidenti e indirizzare i team di risposta agli incidenti nella giusta direzione. La preparazione forense è fondamentale in quanto può distinguere tra un incidente minore e un grave attacco informatico che mette in ginocchio un'azienda.

Il programma CHFI presenta un approccio dettagliato e metodologico alla digital forensics e all'analisi delle prove che ruota anche attorno al Dark Web, all'IoT e al Cloud Forensics.

1. Documenting the Crime Scene
2. Search and Seizure
3. Evidence Preservation
4. Data Acquisition
5. Data Examination
6. Reporting

La versione 11 del corso CHFI include:

- 15 moduli
- 68 laboratori
- Windows 11, Windows Server 2022 e Ubuntu (Linux)

- Nuovi concetti: Computer Forensics Standards, eDiscovery, Wireless...

TARGET

Il programma è progettato per i professionisti IT coinvolti nella sicurezza dei sistemi informativi, nella computer forensics e nella risposta agli incidenti. Amplierà le conoscenze applicative in digital forensics per analisti forensi, investigatori di crimini informatici, analisti forensi di difesa informatica, risponditori di incidenti, revisori di tecnologie dell'informazione, analisti di malware, consulenti di sicurezza e responsabili della sicurezza.

PREREQUISTI

- Conoscenze di base in cyber security, forensic investigation ed incident management.
- Il conseguimento preventivo della certificazione CEH è consigliato.

CONTENUTI

- Modulo 01: Computer Forensics in Today's World
- Modulo 02: Computer Forensics Investigation Process
- Modulo 03: Understanding Hard Disks and File Systems
- Modulo 04: Data Acquisition and Duplication
- Modulo 05: Defeating Anti-Forensics Techniques
- Modulo 06: Windows Forensics
- Modulo 07: Linux and Mac Forensics
- Modulo 08: Network Forensics
- Modulo 09: Malware Forensics
- Modulo 10: Investigating Web Attacks
- Modulo 11: Dark Web Forensics
- Modulo 12: Cloud Forensics
- Modulo 13: Email and Social Media Forensics
- Modulo 14: Mobile Forensics
- Modulo 15: IoT Forensics