Computer Hacking Forensic Investigator (CHFI)

Duration: 5 Days

Course Description:

The Computer Hacking Forensic Investigator (CHFI) course delivers the security discipline of digital forensics from a vendor-neutral perspective. CHFI is a comprehensive course covering major forensic investigation scenarios and enabling students to acquire necessary hands-on experience with various forensic investigation techniques and standard forensic tools necessary to successfully carry out a computer forensic investigation leading to the prosecution of perpetrators.

The CHFI certification gives participants (Law enforcement personnel, system administrators, security officers, defense and military personnel, legal professionals, bankers, security professionals, and anyone who is concerned about the integrity of the network infrastructure.) the necessary skills to perform an effective digital forensics investigation.

CHFI presents a methodological approach to computer forensics including searching and seizing, chain-of-custody, acquisition, preservation, analysis and reporting of digital evidence.

Course Objectives:

- Establish threat intelligence and key learning points to support pro-active profiling and scenario modeling
- Perform anti-forensic methods detection
- Perform post-intrusion analysis of electronic and digital media to determine the who, where, what, when, and how the intrusion occurred
- Extract and analyze of logs from various devices like proxy, firewall, IPS, IDS, Desktop, laptop, servers, SIM tool, router, firewall, switches AD server, DHCP logs, Access Control Logs & conclude as part of investigation process.
- Identify & check the possible source / incident origin.
- Recover deleted files and partitions in Windows, Mac OS X, and Linux
- Conduct reverse engineering for known and suspected malware files
- Collect data using forensic technology methods in accordance with evidence handling procedures, including collection of hard copy and electronic documents

Target Audience:

The CHFI program is designed for all IT professionals involved with information system security, computer forensics, and incident response.

- Police and other law enforcement personnel
- Defense and Security personnel
- e-Business Security professionals
- Legal professionals
- Banking, Insurance, and other professionals
- Government agencies
- IT managers
- Digital Forensics Service Providers

Course Outlines:

- Module 01: Computer Forensics in Today's World
- Module 02: Computer Forensics Investigation Process
- Module 03: Understanding Hard Disks and File Systems
- Module 04: Data Acquisition and Duplication
- Module 05: Defeating Anti-Forensics Techniques
- Module 06: Windows Forensics
- Module 07: Linux and Mac Forensics
- Module 08: Network Forensics
- Module 09: Investigating Web Attacks
- Module 10: Dark Web Forensics
- Module 11: Database Forensics
- Module 12: Cloud Forensics
- Module 13: Investigating Email Crimes
- Module 14: Malware Forensics
- Module 15: Mobile Forensics
- Module 16: IoT Forensics