

Computer Hacking Forensic Investigator

Kód kurzu: CHFI

Na kurze CHFI Computer Hacking Forensic Investigator máte jedinečnú príležitosť získať potrebné znalosti a zoznámiť sa s najnovšími technikami v odbore vyšetrovania počítačových útokov a zaistovania evidencie. Naučíte sa zhromažďovať potrebné dôkazy pre stíhanie útočníkov a správne metódy identifikácie stôp po útočníkoch v prípade napadnutia firmy kybernetickým útokom, či už sa jedná o hromadný útok alebo ojedinelé napadnutie konkrétnej obete. Na tomto školení budeme preberať väčšinu z najnovších nástrojov pre zaistovanie stôp, softwarové či hardwarové nástroje, pomocou ktorých môžete nájsť stopy útočníkov prostredníctvom dát, ktoré zostávajú na napadnutých systémoch, obnovovanie zmazaných, poškodených či kryptovaných súborov, a vypracovať audit, ktorý zabráni budúcim útokom podobného typu. Pretože väčšina útokov je zameraná na dopredu vytipovanú firmu, ide najčastejšie o prípady priemyselnej špionáže, poškodzovania konkurencie či osobného vyrovnávania účtov. Na kurze spoznáte vhodné metódy pre vyšetrovanie kyberútokov, zaistenie dôkazov a stíhanie kyberzločincov. V cene kurzu je i celosvetovo uznávaná skúška EC0 312-49 EC-Council Computer Hacking Forensic Investigator, ktorá dokladá vaše schopnosti vyhľadávania incidentov na všetkých úrovniach od fyzického napadnutia, stop v OS, napadnutia bezdrôtových sietí po útoky na weby.

Komu je kurz určený

Kurz je vhodný pre všetkých, ktorí sa zúčastňujú vyšetrovania kyberútokov a zaistovaní stôp, či už sa jedná o bezpečnostných administrátorov firiem, systémových administrátorov, kriminálnych vyšetrovateľov, alebo súdnych znalcov.

Čo vás naučíme

- Získavať stopy a zaisťovať dôkazy
- Získavať najrôznejšie typy dôkazov z digitálnych médií
- Ako vytvoriť prostredie pre získanie dôkazov
- Rôzne typy súborových systémov a procesy spúšťania systému
- Obnova zmazaných súborov a oddielov vo Windows, Mac OS X a Linuxe
- Techniky steganografie, odhaľovanie steganografie, preskúvanie grafických médií
- Techniky lámania hesiel, nástroje a typy útokov na heslá a preskúvanie súborov chránených heslami
- Rôzne metódy zaistovania dostupnosti logov a nástroje pre ich synchronizáciu a uchovávanie
- Prieskum logov, bezdrôtových útokov a webových útokov
- Sledovanie e-mailovej komunikácie
- Zaistovanie dôkazov z mobilných zariadení
- Vypracovanie vyšetrovacích správ

Požadované vstupné znalosti

Predchádzajúce absolvovanie kurzu Certified Ethical Hacker (CEH) či ekvivalentne veľmi dobré znalosti techník používaných pri penetračnom testovaní firiem.

Osnova kurzu

- Proces forenzného vyšetrovania
- Prehľadávanie a zaistovanie počítačov
- Digitálne dôkazy
- Reakcie na útoky
- Vytváranie laboratórneho prostredia pre zaistovanie dôkazov
- Súborové systémy a preskúvanie diskov
- Vyhľadávanie stôp a zaistovanie dôkazov v OS Windows
- Extrakcie dát a vytváranie kópií
- Obnova zmazaných súborov a oddielov
- Zaistovanie dôkazov pomocou AccessData FTK

GOPAS Praha

Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno

Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava

Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk



Copyright © 2020 GOPAS, a.s.,
All rights reserved

Computer Hacking Forensic Investigator

- Zaisťovanie dôkazov pomocou EnCase
- Steganografia a jej odhaľovanie
- Využívanie nástrojov pre lámanie hesiel
- Zaisťovanie logov a analýza sieťovej prevádzky
- Zaisťovanie útokov na bezdrôtovej sieti
- Zaisťovanie útokov na web
- Zaisťovanie e-mailovej komunikácie, jej vyšetovanie a odhaľovanie zločinov prostredníctvom e-mailu
- Zaisťovanie dôkazov z mobilných telefónov a počítačov
- Vypracovanie vyšetrovacích správ

GOPAS Praha

Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno

Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava

Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk



Copyright © 2020 GOPAS, a.s.,
All rights reserved