Computer Hacking Forensic Investigator

Kód kurzu: CHFI

Na kurzu CHFI Computer Hacking Forensic Investigator máte jedinečnou příležitost získat potřebné znalosti a seznámit se s nejnovějšími technikami v oboru vyšetřování počítačových útoků a zajišťování evidence. Naučíte se shromažďovat potřebné důkazy pro stíhání útočníků a správné metody identifikace stop po útočnících v případě napadení firmy kybernetickým útokem, ať už se jedná o hromadný útok či ojedinělé napadení konkrétní oběti. Na tomto školení budeme probírat většinu z nejnovějších nástrojů pro zjišťování stop, softwarové či hardwarové nástroje, pomocí kterých můžete nalézt stopy útočníků prostřednictvím dat, která zůstávají na napadených systémech, obnovování smazaných, poškozených či kryptovaných souborů, a vypracovat audit, který zabrání budoucím útokům podobného typu. Protože většina útoků je zaměřena na předem vytypovanou firmu, jedná se nejčastěji o případy průmyslové špionáže, poškozování konkurence či osobní vyřizování účtů. Na kurzu poznáte vhodné metody pro vyšetřování kyberútoků, zajištění důkazů a stíhání kyberzločinců.V ceně kurzu je i celosvětově uznávaná zkouška EC0 312-49 EC-Council Computer Hacking Forensic Investigator, která dokládá vaše schopnosti vyhledávání a řešení bezpečnostních incidentů na všech úrovních od fyzického napadení, stop v OS, napadání bezdrátových sítí po útoky na weby.

Pro koho je kurz určen

Kurz je vhodný pro všechny, kdo se účastní vyšetřování kyberútoků a zajišťování stop, ať už se jedná o bezpečnostní administrátory firem, systémové administrátory, kriminální vyšetřovatele nebo soudní znalce.

Co vás naučíme

- Získávat stopy a zajišťovat důkazy
- Získávat nejrůznější typy důkazů z digitálních médií
- Jak vytvořit prostředí pro získávání důkazů
- Různé typy souborových systémů a procesy spouštění systému
- Obnova smazaných souborů a oddílů ve Windows, Mac OS X a Linuxu
- Techniky steganografie, odhalování steganografie prozkoumávání grafických médií
- Techniky lámání hesel nástroje a typy útoků na hesla a prozkoumávání souborů chráněných hesly
- Různé metody zajišťování dostupnosti logů a nástroje pro jejich synchronizaci a uchovávání
- Průzkum logů, bezdrátových útoků a webových útoků
- Sledování e-mailové komunikace
- Zjišťování důkazů z mobilních zařízení
- Vypracování vyšetřovacích zpráv

Požadované vstupní znalosti

Předchozí absolvování kurzu Certified Ethical Hacker (CEH) či ekvivalentní velmi dobré znalosti technik používaných při penetračním testování firem.

Osnova kurzu

- Proces forenzního vyšetřování
- Prohledávání a zajišťování počítačů
- Digitální důkazy
- Reakce na útoky
- Vytváření laboratorního prostředí pro zajišťování důkazů
- Souborové systémy a prozkoumávání disků
- Vyhledávání stop a zajišťování důkazů v OS Windows
- Extrakce dat a vytváření kopií
- Obnova smazaných souborů a oddílů
- Zajištování důkazů pomocí AccessData FTK
- Zajišťování důkazů pomocí EnCase
- Steganografie a její odhalování

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

- Využívání nástrojů pro lámání hesel
- Zajišťování logů a analýza síťového provozu
- Zjišťování útoků na bezdrátové sítě
- Zjišťování útoků na web
- Zajišťování e-mailové komunikace, její vyšetřování a odhalování zločinu prostřednictvím e-mailu
- Zajišťování důkazů z mobilních telefonů a počítačů
- Vypracování vyšetřovacích zpráv

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