

Certified Ethical Hacker v12 PRO

Kód kurzu: CEHv12

Certified Ethical Hacker v12 je nejnovější verze celosvětově nejoblíbenějšího a nejprestižnějšího kurzu firmy EC-Council. Co navíc přináší verze PRO, si přečtěte ZDE. Studenti se v rámci kurzu seznámí se strategiemi, technikami a nástroji, které se běžně používají v aktuálním hackingu a při penetračním testování. Získejte ucelený přehled technik hackingu, jako jsou pokročilá enumerace a skenování sítí či systémů v celopodnikovém rozsahu, tvorba malwaru a trojských koňů, pokročilé síťové útoky eliminující omezení VLAN a jiné techniky. Těšit se můžete na rozšířenou část testování webových serverů a aplikací, SQL Injection či hackování mobilních platforem. V ceně kurzu je i celosvětově uznávaná certifikační zkouška CEH, při které studenti prokazují zvládnutí vyučovaných technik etického hackingu v rámci kurzu. Chraňte Vaše i firemní data!

Materiály ke kurzu

V ceně kurzu jsou zahrnuty oficiální elektronické studijní materiály, přístupy do labů v délce 6 měsíců a voucher na certifikační zkoušku 312-50-ANSI (platnost vouchera je jeden rok od jeho nákupu).

Požadované vstupní znalosti

Zájemci o tento kurz by měli mít alespoň znalosti na úrovni kurzu Network Security - Hacking v praxi (GOC3).

Osnova kurzu

Module 01: Introduction to Ethical Hacking. Cover the fundamentals of key issues in the information security world, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures.

Module 02: Footprinting and Reconnaissance. Learn how to use the latest techniques and tools to perform foot printing and reconnaissance, a critical pre-attack phase of the ethical hacking process.

Module 03: Scanning Networks. Cover the fundamentals of key issues in the information security world, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures.

Module 04: Enumeration. Learn various enumeration techniques, such as Border Gateway Protocol (BGP) and Network File Sharing (NFS) exploits, plus associated countermeasures.

Module 05: Vulnerability Analysis. Learn how to identify security loopholes in a target organization's network, communication infrastructure, and end systems.

Module 06: System Hacking. Learn about the various system hacking methodologies—including steganography, steganalysis attacks, and covering tracks—used to discover system and network vulnerabilities.

Module 07: Malware Threats. Get an introduction to the different types of malware, such as Trojans, viruses, and worms, as well as system auditing for malware attacks, malware analysis, and countermeasures.

Module 08: Sniffing. Learn about packet-sniffing techniques and how to use them to discover network vulnerabilities, as well as countermeasures to defend against sniffing attacks.

Module 09: Social Engineering. Learn social engineering concepts and techniques, including how to identify theft attempts, audit human-level vulnerabilities, and suggest social engineering countermeasures.

Module 10: Denial-of-Service. Learn about different Denial-of-Service (DoS) and Distributed DoS (DDoS) attack techniques, as well as the tools used to audit a target and devise DoS and DDoS countermeasures and protections.

Module 11: Session Hijacking. Understand the various session hijacking techniques used to discover network-level session management, authentication, authorization, and cryptographic weaknesses and associated countermeasures.

Module 12: Evading IDS, Firewalls, and Honeybots. Get introduced to firewall, intrusion detection system, and honeypot

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

Certified Ethical Hacker v12 PRO

evasion techniques; the tools used to audit a network perimeter for weaknesses; and countermeasures.

Module 13: Hacking Web Servers. Learn about web server attacks, including a comprehensive attack methodology used to audit vulnerabilities in web server infrastructures and countermeasures.

Module 14: Hacking Web Applications. Learn about web application attacks, including a comprehensive web application hacking methodology used to audit vulnerabilities in web applications and countermeasures.

Module 15: SQL Injection. Learn about SQL injection attack techniques, injection detection tools, and countermeasures to detect and defend against SQL injection attempts.

Module 16: Hacking Wireless Networks. Learn about wireless encryption, wireless hacking methodologies and tools, and Wi-Fi security tools.

Module 17: Hacking Mobile Platforms. Learn about mobile platform attack vectors, Android vulnerability exploits, and mobile security guidelines and tools.

Module 18: IoT Hacking. Learn about packet-sniffing techniques and how to use them to discover network vulnerabilities, as well as countermeasures to defend against sniffing attacks.

Module 19: Cloud Computing. Learn different cloud computing concepts, such as container technologies and server less computing, various cloud-based threats and attacks, and cloud security techniques and tools.

Module 20: Cryptography. In the final module, learn about cryptography and ciphers, public-key infrastructure, cryptography attacks, and cryptanalysis tools.

Upozorňujeme, že vzhledem k náročnosti obsahu a velkému množství praktických ukázek není možné na kurzu probrat kompletní osnovu, část je určena pouze pro samostudium.

Certikační zkouška CEH

- proktorovaná zkouška, kterou je možné složit v našich testovacích centrech v Praze a Brně
- 125 otázek, správných může být více odpovědí
- délka zkoušky - 4 hodiny
- EC-Council nezveřejňuje, jaká je nutná úspěšnost pro složení zkoušky, celosvětově se pohybuje mezi 60% a 80%

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