

# Certified Ethical Hacker v12 PRO

Kód kurzu: CEHv12

Certified Ethical Hacker v12 je najnovšia verzia celosvetovo najobľúbenejšieho a najprestížnejšieho kurzu firmy EC-Council. Čo navyše prináša verzia PRO, si prečítajte TU. Študenti sa v rámci kurzu zoznámia so stratégiami, technikami a nástrojmi, ktoré sa bežne používajú v aktuálnom hackingu a pri penetračnom testovaní. Získajte ucelený prehľad techník hackingu, ako sú pokročilá enumerácia a skenovanie sietí či systémov v celopodnikovom rozsahu, tvorba malwaru a trójskych koní, pokročilé sieťové útoky eliminujúce obmedzenia VLAN a iné techniky. Tešiť sa môžete na rozšírenú časť testovania webových serverov a aplikácií, SQL Injection či hackovanie mobilných platforiem. V cene kurzu je i celosvetovo uznávaná certifikačná skúška CEH, pri ktorej študenti preukazujú zvládnutie vyučovaných techník etického hackingu v rámci kurzu. Chráňte Vaše i firemné dáta!

Pobočka	Dní	Katalógová cena	ITB
Praha	5	64 900 Kč	75
Brno	5	64 900 Kč	75
Bratislava	5	2 480 €	75

Všetky ceny sú uvedené bez DPH.

## Termíny kurzu

Dátum	Dní	Cena kurzu	Typ výučby	Jazyk výučby	Lokalita
<b>G</b> 21.10.2024	5	64 900 Kč	Prezenčný	CZ/SK	GOPAS Praha
<b>G</b> 11.11.2024	5	2 480 €	Online	CZ/SK	GOPAS Bratislava online
<b>G</b> 11.11.2024	5	64 900 Kč	Online	CZ/SK	GOPAS Praha online
<b>G</b> 16.12.2024	5	64 900 Kč	Prezenčný	CZ/SK	GOPAS Praha
03.02.2025	5	64 900 Kč	Prezenčný	CZ/SK	GOPAS Brno
17.02.2025	5	64 900 Kč	Prezenčný	CZ/SK	GOPAS Praha
07.04.2025	5	64 900 Kč	Prezenčný	CZ/SK	GOPAS Praha
26.05.2025	5	64 900 Kč	Prezenčný	CZ/SK	GOPAS Praha
02.06.2025	5	64 900 Kč	Prezenčný	CZ/SK	GOPAS Brno

Všetky ceny sú uvedené bez DPH.

## Materiály ku kurzu

V cene kurzu sú zahrnuté oficiálne elektronické študijné materiály, prístupy do labov v dĺžke 6 mesiacov a voucher na certifikačnú skúšku vrátane 3 retakov (platnosť vouchera je jeden rok od jeho aktivácie).

## Požadované vstupné znalosti

Záujemcovia o tento kurz by mali mať vedomosti aspoň 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

GOPAS Praha  
Kodaňská 1441/46  
101 00 Praha 10  
Tel.: +420 234 064 900-3  
[info@gopas.cz](mailto:info@gopas.cz)

GOPAS Brno  
Nové sady 996/25  
602 00 Brno  
Tel.: +420 542 422 111  
[info@gopas.cz](mailto:info@gopas.cz)

GOPAS Bratislava  
Dr. Vladimíra Clementisa 10  
Bratislava, 821 02  
Tel.: +421 248 282 701-2  
[info@gopas.sk](mailto:info@gopas.sk)



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

# Certified Ethical Hacker v12 PRO

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 Honeypots.** Get introduced to firewall, intrusion detection system, and honeypot 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 serverless 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 vzhľadom k náročnosti obsahu a veľkému množstvu praktických ukážok nie je možné na kurze prebrať kompletnú osnovu, časť je určená len pre samoštúdium.

**GOPAS Praha**  
Kodaňská 1441/46  
101 00 Praha 10  
Tel.: +420 234 064 900-3  
[info@gopas.cz](mailto:info@gopas.cz)

**GOPAS Brno**  
Nové sady 996/25  
602 00 Brno  
Tel.: +420 542 422 111  
[info@gopas.cz](mailto:info@gopas.cz)

**GOPAS Bratislava**  
Dr. Vladimíra Clementisa 10  
Bratislava, 821 02  
Tel.: +421 248 282 701-2  
[info@gopas.sk](mailto:info@gopas.sk)

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

# Certified Ethical Hacker v12 PRO

## Certifikačná skúška CIEH

- proktorovaná skúška, ktorú je možné zložiť v našom testovacom stredisku
- 125 otázok, správnych môže byť viac odpovedí
- dĺžka skúšky - 4 hodiny
- EC-Council nezverejňuje, aká je nevyhnutná úspešnosť pre zloženie skúšky, celosvetovo sa pohybuje medzi 60 % a 80 %

### **GOPAS Praha**

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

### **GOPAS Brno**

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

### **GOPAS Bratislava**

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



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