# Certified Ethical Hacker v13 ELITE

Kód kurzu: CEHv13

Certified Ethical Hacker (CEH) v13 je nejnovější verzí prestižního kurzu EC-Council pro etické hackery, která přináší zásadní inovace v oblasti kybernetické bezpečnosti. Kurz nyní zahrnuje rozšířené praktické dovednosti a integruje umělou inteligenci (AI) do všech pěti fází etického hackingu, což účastníkům umožňuje efektivnější a modernější přístup k analýze hrozeb a obraně.

| Pobočka | Dnů | Cena kurzu | ITB |
|---|---|---|---|
| Praha | 5 | 64 500 Kč | 50 |
| Brno | 5 | 64 500 Kč | 50 |
| Bratislava | 5 | 2 580 € | 50 |

Uvedené ceny jsou bez DPH.

## Termíny kurzu

| | Datum | Dnů | Cena kurzu | Typ výuky | Jazyk výuky | Lokalita |
|---|---|---|---|---|---|---|
| | 10.08.2026 | 5 | 64 500 Kč | Prezenční | CZ/SK | GOPAS Praha |
| | 07.09.2026 | 5 | 64 500 Kč | Prezenční | CZ/SK | GOPAS Brno |
| | 07.09.2026 | 5 | 2 580 € | Prezenční | CZ/SK | GOPAS Bratislava |
| | 12.10.2026 | 5 | 64 500 Kč | Prezenční | CZ/SK | GOPAS Praha |
| | 16.11.2026 | 5 | 2 580 € | Online | CZ/SK | Online |
| | 14.12.2026 | 5 | 64 500 Kč | Prezenční | CZ/SK | GOPAS Praha |
| | 14.12.2026 | 5 | 2 580 € | Prezenční | CZ/SK | GOPAS Bratislava |

Uvedené ceny jsou bez DPH.

### Materiály ke kurzu

V ceně kurzu jsou zahrnuty:

- oficiální elektronické studijní materiály
- přístupy do labů v délce 6 měsíců
- voucher na prezenční C|EH exam, včetně možnosti jednoho zopakování zkoušky zdarma
- voucher na C|EH Practical
- C|EH Engage - více než 3500 hackerských nástrojů, 519 technik útoků a 220 praktických cvičení. Vyzkoušíte si hackování na reálných cvičeních a získáte další zkušenosti
- C|EH Compete - nové výzvy každý měsíc

### 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.** Learn the fundamentals and key issues in information security, 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 for footprinting and reconnaissance, a critical pre-attack phase of ethical hackingearn.

**Module 03: Scanning Networks.** Learn different network scanning techniques and countermeasures.

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

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk

Copyright © 2026 GOPAS, a.s.,
All rights reserved

**Module 05: Vulnerability Analysis.** Learn how to identify security loopholes in a target organization's network, communication infrastructure, and end systems. Different types of vulnerability assessment and vulnerability assessment tools are also included.

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

**Module 07: Malware Threats.** Learn about different types of malware (Trojan, viruses, worms, etc.), APT and fileless malware, malware analysis procedures, and malware countermeasures tracks.

**Module 08: Sniffing.** Learn about packet sniffing techniques and their uses for discovering network vulnerabilities, plus 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.** Learn 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.** Learn about firewalls, intrusion detection systems (IDS), 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, evasion techniques, and SQL injection countermeasures.

**Module 16: Hacking Wireless Networks.** Learn about different types of encryption, threats, hacking methodologies, hacking tools, security tools, and countermeasures for wireless networks.

**Module 17: Hacking Mobile Platforms.** Learn mobile platform attack vectors, Android and iOS hacking, mobile device management, mobile security guidelines, and security tools.

**Module 18: IoT Hacking.** Learn different types of Internet of Things (IoT) and operational technology (OT) attacks, hacking methodologies, hacking tools, and countermeasures.

**Module 19: Cloud Computing.** Learn different cloud computing concepts, such as container technologies and serverless computing, various cloud computing threats, attacks, hacking methodologies, and cloud security techniques and tools..

**Module 20: Cryptography.** Learn about encryption algorithms, cryptography tools, Public Key Infrastructure (PKI), email encryption, disk encryption, 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.

**GOPAS Praha**
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

**GOPAS Brno**
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

**GOPAS Bratislava**
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk

Copyright © 2026 GOPAS, a.s.,
All rights reserved

# Certified Ethical Hacker v13 ELITE

### Knowledge-based Exam C|EH

- 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 %
- V případě, že si účastník kurzu přeje zkoušku skládat v jiném testovacím středisku Pearson VUE nebo online, je možné voucher za poplatek upgradovat. Aktuální cenu upgradu vám rádi sdělíme, neváhejte nás kontaktovat na adrese info@gopas.cz.

### Practical exam C|EH

- 20 otázek založených na reálných scénářích
- délka zkoušky - 6 hodiny

**GOPAS Praha**
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

**GOPAS Brno**
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

**GOPAS Bratislava**
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk

Copyright © 2026 GOPAS, a.s.,
All rights reserved