

# Certified Penetration Testing Professional


Course code: CPENT

CPENT je nejkročilejší kurz etického hackingu vhodný pro všechny budoucí penetrační testery, bezpečnostní specialisty a pro každého, kde chce mít jistotu, že zvládá techniky etického hackingu prakticky a chce si své zkušenosti nechat potvrdit v praktické certifikaci. Po absolvování kurzu skládáte 24 hodinovou zkoušku skutečného penetračního testování, kde není jen jedna plochá síť, ale celá skupina sítí stejně jako v enterprise prostředí a účastníci musí rozkrýt schéma sítí, provádět hacking různých systémů a pomocí získaných informací se dostat do dalších částí sítí, které jsou ve výchozím stavu nepřístupné. Certifikace CPENT je zaměřena na efektivní provádění penetračního testování v enterprise prostředí. Nejedná se pouze o seznámení s technikami etického hackingu, ale absolventi se naučí správně analyzovat, postupovat a vykonávat proces penetračního testování. Jedinečnost školení a certifikace CPENT spočívá v jeho šíři – pokrývá nejen síťové skenování a enumeraci, penetrační testování Active Directory s hledáním nejčastějších chyb v konfiguraci enterprise systémů, Kerberoastingu a zneužívání NTLM Relay, extrakci dat a prostupováním forestu pomocí Golden Ticketu, testování síťové infrastruktury, webových aplikací s reálnými útoky proti klientům i serverům, mobilních aplikací, ale tento penetrační test také zahrnuje IoT a OT hacking. CPENT je velmi intenzivní kurz etického hackingu pro všechny absolventy certifikace CEH, kteří si chtějí prohloubit praktické znalosti a důkladně se připravit na dvě nejvyšší EC-Council certifikace zároveň: CPENT – Certified Penetration Testing Professional a LPT – Licensed Penetration Tester. Účastníci, kteří získají certifikační skóre nad 90 % získávají nejvyšší certifikační titul LPT. Vzhledem ke svému zaměření a průběhu testu se jedná o ideální přípravu pro všechny, kdo chtějí složit známou a uznávanou certifikační zkoušku OSCP. Na CPENT školení se naučíte reálně provádět testování vzdáleně pomocí vhodně umístěných headless zařízení, kdy reverzní tunely a ověřování pomocí klíčů s minimální možností detekce bude samozřejmostí – naučíte se skenovat prostředí tak, abyste nebyli ihned odhaleni, dále se naučíte správně pracovat s výstupy skenování a analyzovat je tak, abyste uměli vytipovat vhodné cíle pro útok. Kurz zahrnuje i praktické provádění exploitace, které si na kurzu vysvětlíme podrobně včetně praktických cvičení. Samozřejmostí je provedení eskalace privilegií, abyste mohli dosáhnout plného napadení cílů, extrakce všech důležitých informací a pomocí těchto informací prostupovat dále síť pomocí lateral movementu a pomocí pivotingu prostupovat i do sítí, které jsou pro Vás v počáteční fázi penetračního testu nedostupné. Pivoting provádíte nejen pomocí metasploitu, ale také prostřednictvím proxy pivotingu, VPN pivotingu a naučíme se pracovat s předáváním dat mezi více spojení pomocí opomíjených komponent v OS, abyste mohli správně ovládat napadené systémy. Dále se naučíte správně analyzovat webové aplikace a praktickou exploitaci jak web klientů tak web serverů. V další fázi pak prakticky procházíme chyby v bezpečnosti aplikací a způsobu jejich exploitace. Naučíme se také analyzovat IoT firmware tak, abyste našli chybně zakomponované klíče, chyby v komunikaci zařízení a informace o fungování aplikací tak, abyste tato zařízení mohli ovládnout. Seznámíte se také s analýzou OT komunikace. Vzhledem k šíři záběru témat se jedná o velmi intenzivní školení, kterým Vás bude provázet více lektorů pro maximální zefektivnění výuky a předávání praktických zkušeností a vysvětlení nejčastějších chyb v provozním prostředí a aplikacích. Absolvování kurzu CEH a jeho všech požadovaných předešlých kurzů je proto nezbytné minimum. Vzhledem k šíři a hloubce témat silně doporučujeme i předešlé absolvování našich detailních hacking kurzů GOC32, GOC33, GOC54 (případně podrobnějších GOC541 a GOC542) a GOC56, kde účastníci získají velmi detailní praktické zvládnutí principů i praktických technik penetračního testování a na CPENT kurzu, vlastní přípravě i certifikaci se mohli soustředit především na zvládnutí procesu penetračního testování. Po absolvování kurzu si vybíráte mezi skládáním certifikační zkoušky v podobě jednoho 24hodinového online testu nebo 2 online testů v délce 12 hodin a poté do týdne odevzdáváte reálný pentest report. V obou případech se jedná o praktický test pod dohledem, bez rizika podvádění a certifikace dokládá, že jste schopni provádět penetrační testování prakticky. Po absolvování školení, vlastní intenzivní přípravy a certifikace se budete v HackTheBox, během CTF a při provádění pentestingu cítit jako doma.

Affiliate	Duration	Course price	ITB
Praha	5	65 000 Kč	50
Brno	5	65 000 Kč	50
Bratislava	5	2 800 €	50

The prices are without VAT.

## Course terms

Date	Duration	Course price	Type	Course language	Location
<b>GOPAS Praha</b> Na Strži 2097/63 140 00 Praha 4 - Krč Tel.: +420 226 201 390 <a href="mailto:info@gopas.cz">info@gopas.cz</a>		<b>GOPAS Brno</b> Nové sady 996/25 602 00 Brno Tel.: +420 530 513 590 <a href="mailto:info@gopas.cz">info@gopas.cz</a>		<b>GOPAS Bratislava</b> Dr. Vladimíra Clementisa 10 Bratislava, 821 02 Tel.: +421 902 903 132 <a href="mailto:info@gopas.sk">info@gopas.sk</a>	 Copyright © 2026 GOPAS, a.s., All rights reserved

# Certified Penetration Testing Professional

🛡️	29.06.2026	5	65 000 Kč	Presence	CZ/SK	GOPAS Brno
⚙️	13.07.2026	5	2 380 €	Presence	CZ/SK	GOPAS Bratislava
🛡️	20.07.2026	5	65 000 Kč	Presence	CZ/SK	GOPAS Praha
	28.09.2026	5	2 800 €	Presence	CZ/SK	GOPAS Bratislava
	12.10.2026	5	2 800 €	Online	CZ/SK	Online
	02.11.2026	5	65 000 Kč	Presence	CZ/SK	GOPAS Praha
	16.11.2026	5	2 800 €	Presence	CZ/SK	GOPAS Bratislava

The prices are without VAT.

## Pro koho je kurz určen

Tento nejpokročilejší kurz etického hackingu je vhodný pro budoucí penetrační testery, kteří pomocí skutečně uznávaných certifikací dokládají zákazníkům, že zvládají proces penetračního testování prakticky. CPENT je určen také pro IT bezpečnostní specialisty, kteří chtějí prakticky znát problematiku hackingu z širší perspektivy, poznat způsob práce útočníka v napadeném firemním prostředí. CPENT je také kurz vhodný pro všechny, kdo se zajímají o počítačovou bezpečnost a hacking a současně si troufnou na praktickou hacking challenge.

## Co Vás naučíme

Reálně provádět penetrační testování firemní infrastruktury a webových aplikací na úrovni certifikačních zkoušek CPENT, LPT a OSCP

## Požadované vstupní znalosti

Pro absolvování kurzu je naprosto nezbytné zvládnutí technik z kurzu CEH – Certified Ethical Hacker verze 9+

Silně doporučujeme také předchozí absolvování kurzů:

GOC32 – Hacking v Praxi II

GOC33 – Hacking v Praxi III

GOC54 – Zranitelnost webových aplikací (případně podrobnějších a novějších GOC541 a GOC542)

## Studijní materiály

Originální příručka firma EC-Council v podobě e-Courseware

## Osnova kurzu

Průzkum cíle

- OSINT
- Fyzický průzkum a vytipování slabých míst ve fyzickém zabezpečení
- Hardware útoky
- Headless device deployment a management

Skenování a enumerace

- Efektivní využívání nmapu ale i komponent v OS
- DNS extraction
- Průzkum prostředí pomocí pasivní analýzy okolního i vlastního provozu v síti
- Zjišťování topologie sítě a cílových segmentů

Malware deployment

- social engineering
- USB útoky

### GOPAS Praha

Na Strži 2097/63  
140 00 Praha 4 - Krč  
Tel.: +420 226 201 390  
[info@gopas.cz](mailto:info@gopas.cz)

### GOPAS Brno

Nové sady 996/25  
602 00 Brno  
Tel.: +420 530 513 590  
[info@gopas.cz](mailto:info@gopas.cz)

### GOPAS Bratislava

Dr. Vladimíra Clementisa 10  
Bratislava, 821 02  
Tel.: +421 902 903 132  
[info@gopas.sk](mailto:info@gopas.sk)



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

# Certified Penetration Testing Professional

- Obfuscation
- Covert channel

## Pentesting Active Directory

- Kerberos hacking
- Kerberoasting
- NTLM Relay
- Golden Ticket
- Secret data extraction
- Lateral movement

## Pivoting

- Identifikace filtrování komunikace
- Základní pivoting
- Double pivoting
- Manuální postup

## Exploitace

- Reverse engineering
- Fuzzing
- Buffer overflow
- Payload execution

## Privilege escalation

- Analýza konfigurace systémů
- Identifikace aplikací a chyb v konfiguraci
- Zneužívání nalezených chyb

## Web Pentesting

- Enumerace web serveru
- Mapování aplikace
- Exploitace vstupu pomocí injektáže - SQL Injection, Function injection, Object injection
- Local file inclusion
- Remote file inclusion
- Local session poisoning
- Session management
- Remote Code Execution
- Command Execution
- CSRF
- XSS

## IoT Hacking

- Firmware extraction
- Key extraction
- Analýza komunikace

## OT Hacking

- Prostup z IT do OT
- Analýza komunikace
- PLC, Mod Bus

### GOPAS Praha

Na Strži 2097/63  
140 00 Praha 4 - Krč  
Tel.: +420 226 201 390  
[info@gopas.cz](mailto:info@gopas.cz)

### GOPAS Brno

Nové sady 996/25  
602 00 Brno  
Tel.: +420 530 513 590  
[info@gopas.cz](mailto:info@gopas.cz)

### GOPAS Bratislava

Dr. Vladimíra Clementisa 10  
Bratislava, 821 02  
Tel.: +421 902 903 132  
[info@gopas.sk](mailto:info@gopas.sk)



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