Hacking in practice II

Course code: GOC32

V tomto jedinečném a velmi detailním hacking kurzu přinášíme přehled útoků, které jsou pro většinu podnikových sítí nejrizikovější. Kurz vhodně rozšiřuje dlouhodobě nejoblíbenější části školení CEH a do větších detailů probírá část útoků pomocí malware a systémových útoků.Vysvětlíme si, jak často dochází k otevírání podnikové sítě na dálku pomocí malware a trojských koňů a jak lze takový útok zneužít pro kompletní ovládnutí sítě bez fyzického přístupu. V následné části systémových útoků si prokážeme, že staré zvyky správců a chyby ve správě, na kterých stále funguje většina podniků, vedou ke kompletní kompromitaci bez potřeby jakkoli prolamovat přihlašovací údaje a jak obrovsky usnadní přístup údaje získané z paměti a profilů uživatelů. Pro provedení útoků použijeme i falešná USB zařízení, která se naučíte vytvářet za běhu a pomocí kterých můžete ovládnout cizí počítač na dálku a bez vědomí uživatelů i správců jejich počítače připojit do své sítě a odcizit provoz, se kterým můžete i manipulovat. V závěrečné části kurzu se podíváme také do úvodu hackingu mobilních platforem, které lze použít jako platformu pro provedení útoku ale zacílíme si i útoky proti mobilním klientům, které vedou ke kompromitaci našich mobilních zařízení a dat na nich uložených.

Affiliate	Duration	Course price	ITB
Praha	5	35 000 Kč	50
Brno	5	35 000 Kč	50
Bratislava	5	1 500 €	50

The prices are without VAT.

Course terms

	Date	Duration	Course price	Type	Course language	Location
	07.12.2026	5	35 000 Kč	Presence	CZ/SK	GOPAS Brno
	04.01.2027	5	35 000 Kč	Presence	CZ/SK	GOPAS Praha
	18.01.2027	5	35 000 Kč	Online	CZ/SK	Online
	18.01.2027	5	1 500 €	Online	CZ/SK	Online
	01.02.2027	5	1 500 €	Presence	CZ/SK	GOPAS Bratislava
	01.03.2027	5	35 000 Kč	Presence	CZ/SK	GOPAS Brno
	15.03.2027	5	35 000 Kč	Presence	CZ/SK	GOPAS Praha
	03.05.2027	5	1 500 €	Online	CZ/SK	Online
	03.05.2027	5	35 000 Kč	Online	CZ/SK	Online
	17.05.2027	5	1 500 €	Presence	CZ/SK	GOPAS Bratislava
	24.05.2027	5	35 000 Kč	Presence	CZ/SK	GOPAS Praha
	21.06.2027	5	35 000 Kč	Presence	CZ/SK	GOPAS Brno
	02.08.2027	5	35 000 Kč	Presence	CZ/SK	GOPAS Praha
	16.08.2027	5	35 000 Kč	Online	CZ/SK	Online
	16.08.2027	5	1 500 €	Online	CZ/SK	Online
	06.09.2027	5	1 500 €	Presence	CZ/SK	GOPAS Bratislava
	20.09.2027	5	35 000 Kč	Presence	CZ/SK	GOPAS Brno
	11.10.2027	5	35 000 Kč	Presence	CZ/SK	GOPAS Praha
	29.11.2027	5	35 000 Kč	Online	CZ/SK	Online
	29.11.2027	5	1 500 €	Online	CZ/SK	Online
	13.12.2027	5	35 000 Kč	Presence	CZ/SK	GOPAS Praha

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

Hacking in practice II

The prices are without VAT.

Pro koho je kurz určen

Kurz je určen pro správce sítí, administrátory bezpečnost IT, auditorům bezpečnosti a budoucím penetračním testerům, kteří jsou již seznámeni s obsahem základního kurzu GOC3 a chtějí si prakticky vyzkoušet pokročilejší hacking techniky a poznat reálně, na kterých principech funguje napadání a ovládání firemních systémů vzdáleně bez nutnosti přímého zásahu do síťového prostředí, porozumět klíčovým problémům bezpečnosti počítačových sítí jako je sledování našich aktivit na počítači, způsoby ovládání počítačů na dálku a jejich dopady pro bezpečnost firemních dat a celého prostředí. Kurz Vám umožní také pochopit principy útoků pomocí USB zařízení a prakticky se je naučit využívat pro získání kontroly nad vzdáleným počítačem. Kurz je vhodný pro každého, kdo chce do detailu nejen pochopit, ale i prakticky vyzkoušet pokročilejší metody útoků, které zneužívají nejbolestivější chyby, kterých se dopouští většina dnešních IT administrátorů i uživatelů.

Co vás na kurzu naučíme

Tento ojedinělý kurz Vás naučí odhalovat a pro účely penetračního testování využívat nejzávažnější chyby, kvůli kterým lze ovládat firemní prostředích a které reálně ohrožují bezpečnost většiny firem. Naučíme se zneužívat chyby, kterých se dopouští většina pracovníků IT na nejrůznějších pozicích a proč mohou snadno vést ke ztrátě kontroly nad firemní infrastrukturou během systémových útoků. V další části se naučíme jak se vytváří malware pro vzdálené převzetí kontroly nad počítači, sledování aktivit uživatelů, získávání uložených tajemství, skrývání komunikace při ovládání obětí a poznáme, že běžní uživatelé IT prakticky nemají příliš možnost rozpoznat, že se stali obětí útoku spuštění škodlivého kódu ve spustitelných souborech, makrech nebo průstřelem klientské aplikace a nemůžou správně rozpoznat závažnost dopadů útoku. V další části kurzu se naučíme útoky provádět pomocí USB zařízení, která lze zneužít pro přímé napadení systémů a uvidíme, že to ani zdaleka není o USB flash discích, na kterých by měl být malware a naučíme se přímé ovládání komunikace našich USB zařízení. V další části kurzu se naučíte vytvářet kód pro ovládání i na mobilních zařízení a možnost kontroly dat na nich. V závěrečné části se pak věnujeme také problémům DOS útoků, které jsou jedním z důsledků napadání naší infrastruktury stejně tak jako cestou k odstavení klíčové infrastruktury.

Osnova kurzu

Systémové útoky aneb deset nejčastějších hříchů IT pracovníků, kvůli kterým přicházíme o firmu

- Zneužívání nejčastejších chyb v administraci ke kompletní kompromitaci sítě
- Proč nevinné přesměrování lokálních zdrojů v RDP může vést k ovládnutí sítě
- RDP MitM a session recording aneb vzdálený záznam klávesnice a obrazovky admina
- Chybné používání identit pro administraci, spuštění úloh a služeb
- Offline útoky pro ovládnutí domény
- Hesla a vykrádání tajemství z počítačů
- Zneužívání shadowcopy pro vykrádání databází, Active Directory a file serverů
- Zneužívání lokálních účtů ve výchozím nastavení
- Vykrádání paměti počítače
- Vykrádání profilů a šifrovacích tajemství
- Pass The Hash aneb jak s údaji z paměti ovládnout vzdálené systémy a proč není třeba lámat hesla
- NTLM Relay aneb jak položit zcela vzdálené systémy, kam nikdo nechtěl přistupovat jen během útoků MitM
- Responder a podvrh legitimních cílů aneb jak snadno nalákat oběť a zneužít její výchozí nastavení

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

- Pass The Ticket aneb vykrádání Kerberosu
- Kerb roasting aneb kompromitace účtů služeb
- Golden Ticket prakticky - průstřel celého AD forestu pomocí jediné domény
- DMA útoky aneb jak obejít ochranu BitLocker

Malware a vše na co jste se báli zeptat aneb jak ovládnout firmu na dálku a proč je většina firem prostřelená zevnitř

- Princip komunikace a proč útoky zevnitř vedou
- Jak zneužít nejčastější cesty spuštění malwaru k infiltraci prostředí
- Možnosti ovládání a sledování obětí
- Skrývání malware - kam se skrýt, aby vás nikdo nehledal
- Wmi filtry
- Využívání více úrovní streamů
- Opomíjená nastavení office
- Skrývání v registrech
- Šifrování
- Neobvyklé metody spouštění kódu
- Využívání skrytých kanálů a tuneling v jiných protokolech
- Pivoting aneb jak prostoupit z napadeného počítače dál do nepřístupného prostředí
- Automatizace prostupu prostředím
- Infekce obsahu při MitM útocích
- Fileless backdooring
- Asynchronní komunikace
- Skrývání malwaru pomocí Application Compatibility Toolkitu a tvorba shimů

USB Hid útoky aneb jak zneužít cokoli v USB ke kompletní kompromitaci systému

- Falešné USB flash disky dynamicky měnící svůj obsah pro ovládnutí sítě
- Způsob vytváření objektů na HID sběrnici
- Ovládání počítačů pomocí HID injection
- Způsoby zcizení síťového provozu a SSL inspekce
- Přihlášení k systému bez fyzického přístupu
- Reverzní SSH tunel pro ovládnutí počítače
- Kali Nethunter jako penetrační platforma
- P4wnP1 a BashBunny jako prostředek pro penetrační testování

MouseJacking a KeyJacking

- Zneužívání zranitelných klávesnic a myší pro ovládnutí vzdálených počítačů

Úvod do Android Hackingu

- Generování malwaru pro mobilní prostředí
- Prosřelování slabin na zastaralých systémech
- Zneužívání oprávnění aplikací
- Možnosti sledování mobilních zařízení

DoS attacks

- Flooding cílů
- Reflection attacks
- Amplification effect

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