

# Hacking in practice III

Course code: GOC33

V pokročilém kurzu hackingu se zabýváme pokročilými síťovými útoky pro detailní průzkum síťového prostředí. Naučíme se zneužívat slabiny v chybné implementaci zabezpečení ethernet i WiFi sítí. Vyzkoušíme si přístup ochranou sítě na úrovni L2 v podobě VLAN hoppingu i L3 v podobě útoků na routery. Seznámíte se do detailu s možnostmi skenování cílů a to i v situaci, kdy nemáte možnost skenovat cíle napřímo. Seznámíme se s principy nejčastějších webových útoků, které si vyzkoušíme prakticky proti klientům i serverům. Účastníci se seznámí se zneužíváním útoků XSS, Cross Site Request Forgery, SQL injection, blind SQL injection, command injection a dalších. Seznámíme se i s hackingem bezdrátové komunikace pomocí Software Defined Radio a hackingu BluetoothLE. V další části pak využíváme předešlé získané znalosti k analýze a útokům na IoT zařízení, ovládání kamery, žárovky nebo embeded zařízení, takže si ukážeme i hacking HW.

Affiliate	Duration	Course price	ITB
Praha	5	35 000 Kč	75
Brno	5	35 000 Kč	75
Bratislava	5	1 500 €	75

The prices are without VAT.

## Course terms

Date	Duration	Course price	Type	Course language	Location
31.03.2025	5	35 000 Kč	Presence	CZ/SK	Gopas Brno Prezenční
31.03.2025	5	1 500 €	Online	CZ/SK	Gopas Bratislava Online
31.03.2025	5	35 000 Kč	Online	CZ/SK	Gopas Praha Online
22.04.2025	4	31 500 Kč	Presence	CZ/SK	Gopas Praha Prezenční
30.06.2025	5	35 000 Kč	Presence	CZ/SK	Gopas Praha Prezenční

The prices are without VAT.

## Pro koho je kurz určen

Kurz je určen pro správce sítí, pentestery, bezpečnostní auditory a architektky síťové bezpečnosti se znalostmi témat z kurzu GOC3, kteří se chtějí do detailu seznámit s pokročilejšími útoky na síťovou infrastrukturu, prostřelování ochrany rozdělávání sítí do VLAN a alternativními možnostmi Man-in-the-Middle, Software Defined Radio. Kurz je určen také pro všechny, kdo se chtějí prakticky seznámit s metodami webhacking útoků.

## Co vás na kurzu naučíme

Na tomto praktickém kurzu se naučíme pokročilé techniky napadání sítí, obcházet zabezpečení segmentace sítí do VLAN, prostřelit routery oddělující naše síťové segmenty. Naučíme se také testovat bezpečnost podnikových WiFi klientů a infrastruktury. Dále se seznámíme s principy SDR hackingu a útoky na BluetoothLE. Účastníci kurzu se také prakticky seznámí s nejoblíbenějšími webhacking útoky. Tyto nabitě znalosti se potom naučíme uplatňovat při útocích na kamery i IoT a embeded zařízení.

## Osnova kurzu

Pokročilé síťové útoky

- SPAN a RSPAN
- Vlan Hopping

### 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

# Hacking in practice III

- Útoky na 802.1x
- Man in the Middle i bez APR
- Statické zásahy do cache
- Statické zásahy do routingu
- Podvrhávání DHCP serveru
- DHCP Starvation attacks
- DNS spoofing a poisoning
- DNS typy záznamů a chyby v zabezpečení

## Falešná AP a WPA-Enterprise útoky

- Probourávání identit pomocí falešných AP
- Zneužívání falešných AP pro otrávení klientů
- Zneužívání Hosted Networks jako backdoor do podnikového prostředí

## Průzkum síťového prostředí

- Skenování živých cílů i bez nmapu
- Skenování cílů, se kterými nejde komunikovat
- Enumerace aneb zjišťování detailů o napadeném prostředí
- SNMP aneb Security Not My Problem a jak může vést až k podrobení sítě

## Útoky na routery

- Síťové útoky
- Instalace backdoorů do firmware
- Praktické otevření administrace pomocí CSRF útoků
- Přetečení paměti

## Web útoky

- Session Hijacking
- Cross Site Request Forgery
- Cross Site Scripting
- Error Based SQL Injection vs. blind SQL injection
- Command injection
- Click jacking
- Praktické vyzkoušení útoků k ovládnutí klientů, serverů i celkovému otevření sítě

## SDR - Software Defined Radio

- Princip SDR útoků
- Praktické testování SDR
- Útoky na BLE

## IoT hacking

- Statická analýza firmware
- Credential bruteforcing
- Napadání síťové komunikace
- Command injection

### 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