

# Hardening Linux a Windows serverov podľa CIS a STIG

Kód kurzu: LXHARD

V tomto čtyřdenním kurzu účastníci získají teoretické i praktické zručnosti při aplikování doporučení CIS a STIG, auditu a automatizaci hardeningu (Ansible, SCAP nástroje).

Pobočka	Dnů	Cena kurzu	ITB
Praha	4	27 900 Kč	40
Brno	4	27 900 Kč	40
Bratislava	4	1 110 €	40

Uvedené ceny jsou bez DPH.

## Termíny kurzu

Datum	Dnů	Cena kurzu	Typ výuky	Jazyk výuky	Lokalita
🔧 13.07.2026	4	944 €	Prezenční	CZ/SK	GOPAS Bratislava
🔧 📺 31.08.2026	4	23 715 Kč	Teleprezenční	CZ/SK	GOPAS Praha
🔧 📺 31.08.2026	4	23 715 Kč	Teleprezenční	CZ/SK	GOPAS Brno
🔧 📺 31.08.2026	4	944 €	Teleprezenční	CZ/SK	GOPAS Bratislava

Uvedené ceny jsou bez DPH.

## Pro koho je kurz určený

IT administrátoři, bezpečnostní specialisté, DevOps/SecOps inženýři.

## Co Vás naučíme

- Pochopit principy CIS a STIG, rozdíly a použití v praxi.
- Mít schopnost manuálně i automatizovaně hardenovat Linux a Windows servery.
- Mít dovednost v používání auditních nástrojů (OpenSCAP, CIS-CAT, STIG Viewer / SCAP).
- Budete mít hotový Ansible playbook pro hardening a reportovací skripty.

## Požadované vstupní znalosti

Základy správy Linuxu a Windows (práce s příkazovým řádkem, základní GPO/AD znalosti).

## Studijní materiály

Prezentace, PDF osnovy, VM obrazy/virtuální stroje, ukázkové skripty a playbooky, certifikát účasti.

## Osnova kurzu

- Úvod + CIS pro Linux & Windows
- Úvod do hardeningu: principy (minimalizace útočné plochy, least privilege), běžné hrozby a regulace (PCI DSS, NIST).
- Přehled CIS Benchmarks: struktura, Level 1 vs Level 2, jak získat a číst benchmark.
- Příklady doporučení CIS pro Linux i Windows (účty, služby, logování, síť).
- Praktické cvičení: analýza CIS Benchmark (např. Ubuntu a Windows Server) a demo skenování (CIS-CAT Lite/Pro).
- STIG, porovnání STIG vs CIS + pracovní nástroje
- Úvod do STIG (DISA, CAT I-III), SCAP, rozdíly oproti CIS a kdy použít který standard.
- Práce se STIG Viewer a SCAP nástroji, demo SCAP/OSCAP skenování.
- Skupinová aktivita: porovnání konkrétního pravidla (např. politika hesel) v CIS vs STIG.
- Hands-on: Hardening Linux
- Kernel & sysctl, systemd služeb, firewall (firewalld/ufw), správa souborových oprávnění, SELinux/AppArmor.
- Příklady CIS a STIG pravidel pro Linux (vysvětlení a dopad).

### 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

# Hardening Linux a Windows serverov podľa CIS a STIG

- Praktický lab: manuální hardening Ubuntu/RHEL podle CIS Level 1; implementace vybraných STIG CAT I pravidel.
- Ověření shody: OpenSCAP / CIS-CAT skenování a interpretace výsledků.
- Hands-on: Hardening Windows + Ansible automatizace
- Hardening Windows Server (Group Policy, registrace, firewall, Windows Defender), příklady CIS a STIG (SMBv1, audit, ACL).
- Úvod do Ansible (inventory, playbooky) + přehled CIS/STIG rolí a WinRM pro Windows.
- Workshop: vytvoření a spuštění Ansible playbooků — hardening Linux i Windows.
- Závěrečný projekt: nasadit playbook a ověřit compliance (CIS-CAT / OpenSCAP).

#### **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