



Enterprise Computing Solutions - Education Services

## NABÍDKA ŠKOLENÍ

---

**Prosím kontaktujte nás zde**

Arrow ECS, a.s., 28. října 3390/111a, 702 00 Ostrava

Email: [training.ecs.cz@arrow.com](mailto:training.ecs.cz@arrow.com)

Phone: +420 597 488 811



# Check Point Infrastructure Hacking (HackingPoint)

<b>Kód:</b>	<b>DÉLKA:</b>	<b>CENA:</b>
CKT_HPIH	24 Hours (3 DENNÍ)	Kč bez DPH 75,000.00

## Description

Školení je vedeno v anglickém jazyce zahraničním lektorem formou virtuální školení.

Cena školení je 3500 USD bez DPH - tato cena bude při fakturaci přepočtena aktuálním kurzem.

The ideal introductory/intermediate training class designed to teach the fundamentals of what pen testing is all about. This hands-on training was written to address the market need around the world for a real hands-on, practical and hack-lab experience that focuses on what is really needed when conducting a penetration test. Whilst a variety of tools are used, they are the key tools that should be in any penetration tester's kit bag. This, when combined with a sharp focus on methodology will give you what is necessary to start or formalise your testing career.

This entry level web application security testing course is a pre-requisite for the Advanced Infrastructure Hacking course.

## Cíle

- Gain practical experience with tools that will serve you in the future
- Learn core infrastructure techniques
- Go forward into more advanced infrastructure topics

## Určeno pro

- System administrators
- Web developers
- SOC analysts
- Penetration testers
- Network engineers
- Security enthusiasts
- Anyone who wants to take their skills to the next level

## Program

## Day 1

### Infrastructure Basics

- TCP/IP basics
- The art of port scanning
- Target enumeration
- Brute-forcing
- Metasploit basics
- Password cracking

## Day 2

### Hacking Unix, Databases and Applications

- Hacking recent Unix vulnerabilities
- Hacking databases
- Hacking application servers
- Hacking third-party applications (WordPress, Joomla, Drupal)

## Day 3

### Hacking Windows

- Windows enumeration
- Exploiting recent windows vulnerabilities
- Hacking third party software (Browser, PDF, Java)
- Post-exploitation: dumping secrets
- Hacking windows domains

## Termíny školení

Termíny školení na vyžádání, [kontaktujte nás prosím](#)

## Dodatečné informace

Školení je možné zajistit na míru. [Kontaktujte nás pro bližší informace.](#)