



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

Phone: +420 597 488 811



Check Point Advanced Infrastructure Hacking (HackingPoint)

| | | |
|-------------|---------------|---------------|
| Kód: | DÉLKA: | CENA: |
| CKT_HPIHA | 5 (den) | Kč 107,000.00 |

Description

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

Cena školení je 5000 USD bez DPH - tato cena bude při fakturaci přepočtena aktuálním kurzem.

This Advanced Infrastructure Hacking class is designed for those who wish to push their knowledge. The fast-paced class teaches the audience a wealth of hacking techniques to compromise various operating systems and networking devices. The class will cover advanced penetration techniques to achieve exploitation and will familiarize you with hacking of common operating systems, networking devices and much more. From hacking domain controllers to local root, VLAN hopping to VoIP hacking, we have got everything covered.

Cíle

Understanding Advanced Hacking techniques for infrastructure devices and systems, is critical for penetration testing, red teaming, and managing vulnerabilities in your environment.

Students will become familiar with hacking techniques for common operating systems and networking devices.

Určeno pro

Those taking Crest CCT (ICE), CHECK (CTL), TIGER SST, and other similar industry certifications.

Those who perform penetration testing on infrastructure and want to add to their existing skill set.

Vstupní znalosti

Laptop and with admin/root access.

Experience with common hacking tools such as Metasploit is recommended, but not a requirement.

Program

Day 1

IPv4 and IPv6 refresher

- Advanced topics in network scanning
- Understanding and exploiting IPv6 targets
- OSINT, DVCS exploitation
- Advanced OSINT data gathering
- Exploiting git and continuous integration (CI) servers

Database servers

Database servers

- MySQL
- Postgres
- Oracle

Recent vulnerabilities

- Heart-Bleed and Shell-Shock
- PHP serialization exploit
- Web-sphere Java exploits

Day 2

Windows exploitation

- Domain and user enumeration
- AppLocker/GPO restriction bypass
- Local privilege escalation
- Post exploitation #1 (AMSI bypass & Mimikatz)
- Post exploitation #2 (LSASecrets)

Day 3

AD exploitation

- Active Directory delegation issues
- WOW64
- Pivoting and WinRM
- Persistence (Golden Ticket and DCSync)
- Lateral movement using WMIC

Day 4

Linux exploitation

- Port scanning and enumeration
- FS + SSH
- Privilege escalation
- Rservices
- Apache
- X11 services

Day 5

Container breakout

Container breakout

Docker breakout

VLAN exploitation

VLAN concepts

VLAN hopping attacks

VPN exploitation

VPN

VoIP exploitation

VoIP enumeration

VoIP exploitation

Termíny školení

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

Dodatečné informace

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