



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



Kód:	DÉLKA:	CENA:
OTH_GOC3	40 Hours (5 dní)	Kč 34,500.00

Description

Toto školení hackingu vás seznámí se základními nástroji a principy, které se používají pro útoky a penetrační testování. Náš ojedinělý pětidenní kurz vám umožní do detailu pochopit i vyzkoušet metody, pomocí kterých se provádí útoky na počítačové sítě a serverové systémy z vnitřní části sítě a při útocích Man-in-the-Middle proti klientům mimo vnitřní síť. Účastníci si vyzkouší řadu technik jak na Windows platformě, tak i na Linuxu. Účast na tomto kurzu nebo odpovídající znalosti jsou nutným předpokladem pro účast na kurzu CEHv8 - Certified Ethical Hacker.

UPOZORNĚNÍ K CENĚ KURZU:

Cena školení pořádaného v Bratislavě (slovensky) je 1050 EUR bez DPH - tato cena bude při fakturaci přepočtena aktuálním kurzem.

Toto školení pořádá společnost GOPAS a.s.

Cíle

Náš ojedinělý kurz GOC3 Hacking v praxi Vám umožní do detailu pochopit i vyzkoušet metody, pomocí kterých se provádí útoky na naše počítačové sítě a serverové systémy. V průběhu kurzu si postupně vysvětlíme i vyzkoušíme vše, co potřebujete znát pro obranu proti technikám pro mapování prostředí napadených firem, skenování síťového prostředí, ARP poisoning, ukládání a přenos hesel v síti a metody pro jejich zachytávání a prolamování pomocí CPU, GPU a distribuovaného útoku. V následující části kurzu probíráme slabiny bezdrátových sítí, kde si vysvětlíme jednotlivé druhy provozu ve WiFi sítích a máte možnost si prakticky vyzkoušet monitorování WiFi sítí i techniky generování síťového provozu pomocí WiFi injection, odpojování klientů v síti, zachytávání provozu v monitorovacím módu a prolamování hesel do WEP a WPA sítí. V závěrečné části kurzu si ukážeme také pokročilé útoky Man in the Middle, které se dnes používají pro eliminaci zabezpečení HTTPS, co hrozí na nezáplatovaných systémech - napadání počítačových systémů pomocí obávané exploitace služeb a metody skrývání v napadeném systému.

Určeno pro

Kurz je určen správcům sítí, kteří jsou zodpovědní za bezpečnost počítačových sítí a chtějí pomocí praktických ukázek porozumět, proč je nutné zavádět opatření, které standardní bezpečnostní kurzy a oficiální whitepapery vysvětlují pouze teoreticky. Kurz můžeme doporučit i správcům síťové infrastruktury pro hlubší porozumění principům TCP/IP protokolu. Díky úvodní části opakování TCP/IP se kurzu mohou účastnit všichni, kdo již mají znalosti a zkušenosti na úrovni kurzu GOC2 nebo alespoň roční zkušenosti s administrací síťových služeb a znalosti základní správy serverových operačních systémů. V průběhu kurzu používáme nástroje pro Windows i jejich ekvivalenty v Linux prostředí, avšak díky detailním vysvětlením i instrukcím v průběhu kurzu znalost linux systému není zapotřebí.

Program

Úvod

- Opakování TCP/IP
- Odchytávání dat v síťovém analyzáru
- Vyhledávání informací z Internetových zdrojů
- Spouštění procesů pod službami a plánovanými úlohami

Analýza prostředí a první útoky

- Analýza prostředí náchylných k sociálnímu inženýrství
- Skenování síťových služeb pomocí skenování otevřených portů a bannerů
- Analýza používaných operačních systémů
- Princip a aplikování ARP poisoningu pomocí nástrojů pro Microsoft Windows i Linux

Hesla a jejich prolamování

- Principy ukládání hesel v operačních systémech
- Přenos hesel při síťovém ověřování
- Downgrade ověřovacích metod
- Útoky na hesla hrubou silou pomocí CPU, grafických karet a distribuovaného útoku
- Rainbow Tables - principy vyhledávání, způsob generování pro konkrétní prostředí a druhy útoků, analýza time/memory tradeoff efektu

Bezdrátové sítě

- Druhy rámců používaných v bezdrátových sítích
- Analýza bezdrátových sítí v dosahu
- Zneužití neautorizovaných rámců
- WiFi Injection a monitor mód WiFi karet
- Útoky na WEP sítě
- Útoky na WPA1 PSK a WPA2 PSK sítě
- Prolamování EAPOL rámců pomocí grafických karet
- Vetřelecká AP
- WPS

Pokročilejší útoky

- Zasílání falešných certifikátů, importování kořenových certifikačních autorit a vytváření legitimních falešných certifikátů obcházení HTTPS zabezpečení
- Využití Metasploit Frameworku pro exploitaci síťových služeb
- Skrývání prostředků pomocí rootkitů

Termíny školení

Datum	Místo konání	Časové pásmo	Jazyk	Typ	Garance termínu	CENA
17 Apr 2023	Praha	CEDT	English	Classroom		Kč 34,500.00
12 Jun 2023	Praha	CEDT	English	Classroom		Kč 34,500.00

Dodatečné informace

Školení je možné zajistit na míru. Kontaktujte nás pro bližší informace.