CompTIA PenTest+

Course code: CTPEN

Kurz je určen bezpečnostním specialistům a administrátorům, kteří chtějí začít s penetračním testováním nebo chtějí znát problematiku penetračního testování a seznámit se s postupy, které používají etičtí hackeři při penetračních testech. Kurz je určen také těm administrátorům, kteří sami testovat nebudou, ale chtějí nebo potřebují znát penetrační testování i z druhé strany. Lépe tak pochopí opatření, která by měli přijmout pro zvýšení míry zabezpečení svých sítí.
Kurz je zároveň přípravou na certifikační zkoušku CompTIA PenTest+ (není součástí kurzu).

Pro koho je kurz určený

Kurz je určen bezpečnostním specialistům a administrátorům, kteří chtějí pochopit problematiku penetračního testování a seznámit se s postupy, které používají etičtí hackeři při penetračních testech. Kurz je určen také těm administrátorům, kteří sami testovat nebudou, ale chtějí nebo potřebují znát penetrační testování i z druhé strany. Lépe tak pochopí opatření, která by měli přijmout pro zvýšení míry zabezpečení svých sítí.

Co Vás naučíme

Naučíte se, jak plánovat a vykonávat penetrační test s cílem identifikovat slabá místa, následně analyzovat získané informace a navrhnout potřebná opatření. Získáte znalosti a dovednosti, které budou pevným základem pro váš vstup do světa penetračních testů.
Kurz je zároveň přípravou na certifikační zkoušku CompTIA PenTest+ (není sopučástí kurzu).

Požadované vstupní znalosti

Znalosti na úrovni kurzu CompTIA Security+.

Studijní materiály

The Official CompTIA PenTest+ Student Guide (Exam PT0-002).

Osnova kurzu

Požadavky organizací

- Definování penetračního testu
- Porovnání standardů a metod
- Vyhodnocení požadavků
- Příprava dokumentace

Stanovení a vyhodnocení cílů

- Získání základních informací
- Sběr informací z webu
- OSINT

Lidské a fyzické slabiny

- Zneužití lidské psychiky
- Shrnutí fyzických útoků
- Nástroje na sociálně-inženýrské útoky

Příprava na skenování slabin

- Plánování vyhledávání slabin
- Identifikace obranných prvků
- Nástroje na skenovaní

Skenování

- Skenování identifikovaných cílů
- Vyhodnocení síťové komunikace

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

- Identifikování wifi zařízení

Analýza výsledků skenování
- NMAP
- Analýza výstupů ze skenování

Jak se bránit
- Vyhnutí se detekci
- Steganografie
- Vytvoření skrytého kanálu C&C

Zneužití sítě a cloudu
- Seznam zařízení
- Útok na LAN protokoly
- Nástroje na zneužití
- Odhalení slabin cloudu
- Útoky na cloud

WiFi sítě
- Útoky na wifi sítě
- Nástroje

Mobilní zařízení
- Slabiny mobilních zařízení
- Útoky na mobilní zařízení
- Nástroje

Útoky na jiné systémy
- IoT
- Slabiny virtuálních počítačů

Webové aplikace
- Slabiny webů
- Útok na spojení
- Modifikace dat
- Nástroje

Útoky na systémy
- Vzdálený přístup
- Analýza kódu

Testování přihlašovacích údajů

Sumarizace a reporty

Doporučená opatření
- Technická opatření
- Administrativní a operační opatření
- Fyzická opatření

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk