CompTIA PenTest+ - úvod do penetračného testovania

Kód kurzu: CTPEN

Kurz je určený bezpečnostným špecialistom a administrátorom, ktorí chcú začať s penetračným testovaním alebo chcú poznať problematiku penetračného testovania a zoznámiť sa s postupmi, ktoré používajú etickí hackeri pri penetračných testoch. Kurz je určený aj tým administrátorom, ktorí neplánujú vykonávať penetračné testy, ale chcú veci vidieť aj z druhej strany, aby lepšie chápali opatrenia, ktoré by mali prijímať pri zvyšovaní miery zabezpečenia svojich sietí. Kurz je zároveň prípravou na certifikačnú skúšku CompTIA PenTest+ (nie je súčasťou kurzu).

Pre koho je kurz určený

Kurz je určený bezpečnostným špecialistom a administrátorom, ktorí chcú poznať problematiku penetračného testovania a zoznámiť sa s postupmi, ktoré používajú etickí hackeri pri penetračných testoch. Kurz je určený aj tým administrátorom, ktorí neplánujú vykonávať penetračné testy, ale chcú veci vidieť aj z druhej strany, aby lepšie chápali opatrenia, ktoré by mali prijímať pri zvyšovaní miery zabezpečenia svojich sietí.

Čo Vás naučíme

Účastníci sa naučia plánovať a vykonať penetračný test s cieľom identifikovať slabé miesta a následne analyzovať získané informácie a navrhnúť potrebné opatrenia. Získate zručnosti a znalosti, ktoré budú solídnym základom pre váš vstup do sveta penetračných testerov.

Kurz je zároveň prípravou na certifikačnú skúšku CompTIA PenTest+ (nie je súčasťou kurzu).

Požadované vstupné znalosti

Znalosti na úrovni kurzu CompTIA Security+

Študijné materiály

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

Osnova kurzu

Požiadavky organizácie

- Definovanie penetračného testu
- Porovnanie štandardov a metód
- Vyhodnotenie požiadaviek
- Príprava dokumentácie

Určenie a spoznanie cieľa

- Získanie základných informácií
- Zber informácií z webu
- OSINT

Ľudské a fyzické slabiny

- Zneužitie ľudskej psychiky
- Sumarizácia fyzických útokov
- Nástroje na sociálno-inžinierske útoky

Príprava skenovania slabín

- Plánovanie vyhľadávania slabín
- Identifikácia obranných prvkov
- Nástroje na skenovanie

Skenovanie

- Skenovanie identifikovaných cieľov
- Vyhodnotenie sieťovej komunikácie

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

- Identifikovanie wifi zariadení

Analýza výsledkov skenovania
- NMAP
- Analýza výstupov zo skenovania

Ako sa skryť
- Vyhnutie sa zdetekovaniu
- Steganografia
- Vytvorenie skrytého kanálu C&C

Zneužitie siete a cloudu
- Zoznam zriadení
- Útok na LAN protokoly
- Nástroje na zneužitie
- Odhalenie slabín cloudu
- Útoky na cloud

WIFI siete
- Útoky na wifi siete
- Nástroje

Mobilné zariadenia
- Slabiny mobilných zariadení
- Útoky na mobilné zariadenia
- Nástroje

Útoky na iné systémy
- IoT
- Slabiny virtuálnych počítačov

Webové aplikácie
- Slabiny webov
- Útok na spojenie
- Modifikácia dát
- Nástroje

Útoky na systémy
- Vzdialený prístup
- Analýza kódu

Testovanie prihlasovacích údajov

Sumarizácia a reporty

Odporúčanie opatrení
- Technické opatrenia
- Administratívne a operačné opatrenia
- Fyzické opatrenia

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