securitum

SECURITUM
NET EXPERT

NAJBARDZIEJ PRAKTYCZNY
I KOMPLEKSOWY KURS
Z BEZPIECZEŃSTWA SIECI IT
NA RYNKU!

DWA SZKOLENIA

~~5049~~ ZŁ NETTO

3599 ZŁ NETTO

MODUŁ 1

Bezpieczeństwo sieci/ testy penetracyjne

3 dni szkoleniowe*

* Każdy z modułów można kupić odrębnie

MODUŁ 2

Zaawansowane bezpieczeństwo sieci

2 dni szkoleniowe*

* Każdy z modułów można kupić odrębnie

DLACZEGO TEN KURS JEST TAK DOBRY

- Łącznie aż 5 dni praktycznej, warsztatowej wiedzy
- Minimum niezbędnej teorii, realne przykłady luk w zabezpieczeniach sieci, skuteczne sposoby ich eliminacji
- Wiedza zdobywana od doświadczonych administratorów/audytorów systemów IT
- Dostęp do dedykowanej platformy szkoleniowej i laboratorium sieciowego
- Certyfikat uczestnictwa w szkoleniu (w językach polskim i angielskim)

KORZYŚCI DLA FIRMY I ZESPOŁU

SKUTECZNIEJSZA identyfikacja potencjalnych ataków na infrastrukturę sieciową firmy

MOŻLIWOŚĆ zastosowania poznanych metod ochrony przed atakami

UMIEJĘTNOŚĆ samodzielnego przeprowadzenia testów penetracyjnych infrastruktury i aplikacji

WZROST ŚWIADOMOŚCI zespołu w zakresie skutków cyberprzestępstw

ZWIĘKSZENIE BEZPIECZEŃSTWA w firmie

https://netexpert.securitum.pl/

AGENDA

MODUŁ 1

BEZPIECZEŃSTWO SIECI/TESTY PENETRACYJNE

- Wstęp – elementy bezpieczeństwa informacji
- Testy penetracyjne – jako metoda testowania bezpieczeństwa sieci
- Modyfikacja komunikacji sieciowej
- Bezpieczeństwo sieci – Ethernet
- Bezpieczeństwo warstwy 3 modelu OSI
- Firewalle
- Bezpieczeństwo IPsec
- Bezpieczeństwo protokołów routingu
- Bezpieczeństwo web
- Systemy klasy IPS (Intrusion Prevention System) oraz firewalle aplikacyjne
- Podatności klasy *buffer overflow*
- Realizacja przykładowego testu penetracyjnego w LAB-ie

MODUŁ 2

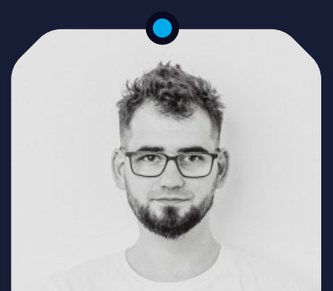
ZAAWANSOWANE BEZPIECZEŃSTWO SIECI

- Zamiast wstępu – pokaz na żywo ataku na urządzenie sieciowe, które... ma zapewnić bezpieczeństwo w firmie (!)
- Praktyczny przegląd aktualnych/ciekawych podatności w infrastrukturze IT
- Pokaz ataku na infrastrukturę IT. Praktyczne demo, jak hackerzy przejmują organizację
- Wybrane zagadnienia bezpieczeństwa aplikacji mobilnych
- Bezpieczeństwo Dockera. Jak korzystać z tego środowiska w sposób bezpieczny
- Wybrane zagadnienia bezpieczeństwa Cloud
- Praktyczny test bezpieczeństwa – samodzielne wyszukiwanie podatności w infrastrukturze sieciowej

DLA KOGO

- Administratorzy IT
- Pentesterzy
- Osoby odpowiedzialne za wdrożenia zabezpieczeń w firmach
- Pracownicy działów bezpieczeństwa
- Pracownicy SOC

TRENERZY



Maciej Szymczak jest konsultantem ds. bezpieczeństwa IT w Securitum. Ex-admin, z ponaddziesięcioletnim doświadczeniem zrealizowanym od patchcordu po BGP, od Gentoo ze stage1 po Ansible na tysiącach serwerów... Od 2017 roku pentester/audytor badający bezpieczeństwo sieci i aplikacji największych podmiotów na rynku. Pasjonat bezpieczeństwa informacji z zacięciem do przekazywania wiedzy.

Marek Rzepecki to pasjonat tematyki cyberbezpieczeństwa, konsultant ds. bezpieczeństwa IT w Securitum. W ciągu kilku ostatnich lat zrealizował ponad 250 niezależnych audytów bezpieczeństwa aplikacji webowych i mobilnych, infrastruktur sieciowych oraz ataków DDoS dla polskich oraz zagranicznych firm. Aktywny bug bounter, prelegent na konferencjach branżowych, współautor książki *Wprowadzenie do bezpieczeństwa IT*.

ZAPISY I SZCZEGÓŁY

https://netexpert.securitum.pl/

Dodatkowe pytania: Aneta Jandziś
aneta.jandzis@securitum.pl
tel. +48 (12) 352 33 82
516 824 029