Testy penetracyjne i testowanie bezpieczeństwa sieci (kod: Testy penetracyjne)

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl

Opis i cel szkolenia

Szkolenie ma na celu dostarczenie uczestnikom kompleksowej wiedzy i praktycznych umiejętności z zakresu testowania bezpieczeństwa sieci oraz przeprowadzania testów penetracyjnych. Program kursu został zaprojektowany tak, aby uczestnicy mogli zdobyć zarówno teoretyczne, jak i praktyczne umiejętności niezbędne do skutecznego identyfikowania i zarządzania zagrożeniami bezpieczeństwa w sieciach komputerowych.

Szkolenie zawiera elementy praktyczne, w tym ćwiczenia z wykorzystaniem symulowanych środowisk testowych, które pozwolą uczestnikom na zdobycie praktycznego doświadczenia. Omówione zostaną studia przypadków rzeczywistych ataków i incydentów, które pomogą w zrozumieniu wyzwań i najlepszych praktyk w branży.

Czas trwania

2 dni

Program

1. Wprowadzenie do testów penetracyjnych:
   — Omówienie różnych podejść i metod stosowanych w testach penetracyjnych.
   — Standardy OSSTMM i OWASP - przegląd standardów i wytycznych jako podstaw do prowadzenia testów.
   — Dobre praktyki opisane w dokumentach NIST i CIS - prezentacja dokumentów, które zawierają rekomendacje dotyczące zabezpieczeń.
   — Wyjaśnienie kluczowych różnic między testami penetracyjnymi a audytami bezpieczeństwa
2. Organizacja testów penetracyjnych:
   — Prawne aspekty przeprowadzania testów penetracyjnych
   — Tworzenie skutecznego i szczegółowego planu testów penetracyjnych.
   — Rozwiązywanie popularnych problemów napotykanych podczas testów
3. Fazy testu penetracyjnego:
   — Rekonesans i techniki zbierania informacji
   — Metody identyfikacji słabości i podatności w systemach
   — Praktyczne aspekty przeprowadzania ataków na cele testowe
   — Techniki ukrywania śladów po przeprowadzonych testach
   — Tworzenie kompleksowego raportu z przeprowadzonych testów, zawierającego rekomendacje
4. Metody ochrony przed atakami:
   — Zastosowanie i konfiguracja honeypotów jako narzędzi do wykrywania ataków.
   — Omówienie systemów detekcji i prewencji włamań (IDS/IPS)
   — Hardening systemów Windows i Linux - techniki wzmacniania zabezpieczeń systemów operacyjnych

Przeznaczenie i wymagania

Szkolenie jest przeznaczone dla specjalistów ds. bezpieczeństwa IT, administratorów sieci, audytorów IT oraz wszystkich osób odpowiedzialnych za zarządzanie bezpieczeństwem sieci w organizacjach. Uczestnicy powinni posiadać podstawową wiedzę z zakresu sieci komputerowych oraz bezpieczeństwa informatycznego.

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl

Certyfikaty

Uczestnicy szkolenia otrzymują imienne certyfikaty sygnowane przez ALX.

Lokalizacje

— Warszawa – ul. Jasna 14/16A
— Zdalnie – zajęcia realizowane poprzez platformę Zoom
— Kraków – ul. św. Filipa 23
— Katowice – ul. Stawowa 10
— Wrocław – ul. Rynek 35
— Gdańsk – ul. Toruńska 12
— Warsaw (English) – Jasna 14/16A
— Online (English) – your home, office or wherever you want
— na życzenie dowolne miejsce w Polsce, lub UE (zajęcia prowadzone w języku angielskim)

Cena szkolenia

2490 PLN netto (VAT 23%)

W cenę szkoleń organizowanych w naszej siedzibie wliczone są:

— autorskie materiały szkoleniowe,
— indywidualne stanowisko komputerowe do pracy podczas zajęć,
— certyfikaty ukończenia szkolenia,
— drobny poczęstunek oraz ciepłe i zimne napoje,
— możliwość jednorazowego kontaktu z instruktorem (instruktorami) po szkoleniu i zadawania pytań dotyczących materiału szkolenia.

Cena szkolenia nie zawiera obiadów. Można je dokupić w cenie 35 zł netto za obiad.