Możliwość dofinansowania

Szkolenie PEN-200 Penetration Testing with Kali Linux - kompleksowy kurs e-learningowy

Numer usługi 2026/07/20/142469/3697874

7 870,77 PLN brutto
6 399,00 PLN netto
24,52 PLN brutto/h
19,93 PLN netto/h
261,33 PLN cena rynkowa

SOFTRONIC SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

4,3 / 5

197 ocen

Usługa szkoleniowa
zdalna
321:00 h
21.09.2026 do 19.12.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie PEN-200 Penetration Testing with Kali Linux jest skierowane do osób, które chcą rozpocząć karierę profesjonalnego testera penetracyjnego lub chcą zdobyć umiejętności wymagane przez testerów penetracyjnych. Szkolenie w języku angielskim.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	5
Data zakończenia rekrutacji	01-09-2026
Forma prowadzenia usługi	zdalna
Podstawa uzyskania wpisu do BUR	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Celem kursu jest przygotowanie uczestników do samodzielnego identyfikowania i wykorzystywania rzeczywistych luk w zabezpieczeniach komputerów, sieci, aplikacji internetowych i podstawowych środowiskach chmurowych niezbędnego do symulowania ofensywnych operacji bezpieczeństwa — i obrony przed nimi.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Opisuje koncepcje, technologie i najlepsze praktyki stanowiące fundament bezpieczeństwa informacji.	Definiuje podstawowe pojęcia dot. cyberbezpieczeństwa	Test teoretyczny z wynikiem generowanym automatycznie
	Opisuje modele bezpieczeństwa	Test teoretyczny z wynikiem generowanym automatycznie
	Wymienia zagrożenia bezpieczeństwa informacji	Test teoretyczny z wynikiem generowanym automatycznie
	Opisuje dobre praktyki bezpieczeństwa informacji	Test teoretyczny z wynikiem generowanym automatycznie
Identyfikuje podatności	Opisuje techniki i narzędzia etycznego hakowania, takie jak Nmap i Shodan.	Test teoretyczny z wynikiem generowanym automatycznie
	Opisuje narzędzie wykorzystywane do skanowania podatności.	Test teoretyczny z wynikiem generowanym automatycznie
	Wyjaśnia słabości architektoniczne web aplikacji, które stanowią typowe wektory ataków na bezpieczeństwo sieci	Test teoretyczny z wynikiem generowanym automatycznie
Eksploatuje podatności w aplikacjach webowych	Opisuje podstawowe strategie zapobiegania typowym atakom internetowym, lukom w zabezpieczeniach, przechwytywaniu sesji	Test teoretyczny z wynikiem generowanym automatycznie
	Opisuje najczęstsze wektory ataku	Test teoretyczny z wynikiem generowanym automatycznie
	Wyjaśnia mechanizm manipulowania bazami danych za pomocą SQL Injection	Test teoretyczny z wynikiem generowanym automatycznie
	Opisuje luki w zabezpieczeniach przeglądarek internetowych, rozszerzenia przeglądarek i technologie po stronie klienta, które pozwalają włamać się do systemów użytkowników i uzyskać do nich dostęp.	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Identyfikuje błędne konfiguracje i luki w zabezpieczeniach systemów Windows/Linux/AD	Identyfikuje i wykorzystuje błędne konfiguracje i luki w zabezpieczeniach systemów Windows/Linux	Test teoretyczny z wynikiem generowanym automatycznie
	Opisuje strukturę usługi Active Directory	Test teoretyczny z wynikiem generowanym automatycznie
	Wykorzystuje narzędzia takie jak BloodHound i PowerView w celu identyfikowania ścieżek ataków	Test teoretyczny z wynikiem generowanym automatycznie
Tworzy profesjonalne raporty wyników testów	Opisuje wyniki testów w formie zrozumiałych rekomendacji biznesowych	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Kurs **Penetration Testing with Kali Linux (PEN-200)** to podstawowy program szkoleniowy OffSec dla przyszłych testerów penetracyjnych. W trakcie szkolenia uczestnicy dowiedzą się jak identyfikować i wykorzystywać rzeczywiste luki w zabezpieczeniach komputerów, sieci, aplikacji internetowych i podstawowych środowiskach chmurowych. Kładąc nacisk na praktyczną naukę, PEN-200 zapewnia podstawowe umiejętności techniczne i nastawienie niezbędne do symulowania ofensywnych operacji bezpieczeństwa informacji i obrony przed nimi. Jest to kluczowe źródło wiedzy dla osób ubiegających się o stanowiska takie jak analityk bezpieczeństwa, specjalista ds. bezpieczeństwa lub certified ethical hacker.

Szkolenie realizowane jest w formule **e-learningu asynchronicznego** (self-paced) **w języku angielskim**.

Uczestnik otrzymuje dostęp do indywidualnie wygenerowanego konta **na platformie OffSec** na okres **90 dni.**W tym czasie może korzystać z materiałów bez narzuconych terminów i godzin nauki, dostosowując tempo oraz harmonogram nauki do własnej dyspozycyjności.

Walidacja: Na koniec usługi Uczestnik wykonuje post-test w celu dokonania oceny wzrostu poziomu wiedzy (test teoretyczny z wynikiem generowanym automatycznie).

Penetration Testing with Kali Linux (PEN-200) e-learning

- 90 dni dostępu do kursu i laboratoriów praktycznych **na platformie OffSec**
- Jedno podejście do egzaminu certyfikacyjnego wliczone w cenę.
- Ponad 50 laboratoriów Proving Grounds Play – symulacje ataków w realistycznym środowisku.
- Bonusowy dostęp do kursu PEN-103, umożliwiający zdobycie dodatkowego certyfikatu.

Struktura szkolenia:

Kurs PEN-200 składa się **z ponad 20 modułów tematycznych**, obejmujących łącznie **321 godz**.

Większość modułów zawiera filmy instruktażowe.

Większość modułów obejmuje ćwiczenia laboratoryjne, które pomagają uczestnikom przećwiczyć koncepcje i teorię omawianą w danym module.

Po opanowaniu wszystkich technik i umiejętności omawianych we wszystkich modułach, uczestnicy mogą przejść do laboratoriów testowych, aby przećwiczyć kombinację umiejętności w jednym laboratorium, naśladując rzeczywiste doświadczenie w teście penetracyjnym.

Aby pomóc uczestnikom w przygotowaniu się do egzaminu OSCP+, zaprojektowano również laboratoria testowe, które wiernie odzwierciedlają środowisko egzaminacyjne OSCP+.

Program szkolenia:

Podstawy testów penetracyjnych

Poznanie kluczowych pojęć, modeli zagrożeń i etycznych zasad testów penetracyjnych, aby zbudować solidne podstawy wiedzy.

Metodyka ataku i obrona

Omówienie cyklu ataku (recon, exploit, post-exploit) oraz zasad obrony i minimalizacji ryzyka podczas testów.

Planowanie i przygotowanie testów

Opracowanie planu testów: zakresu, reguł zaangażowania, zgód i przygotowania środowiska testowego.

Przegląd narzędzi ofensywnych

Zapoznanie się z zestawem narzędzi pentesterskich i kryteriami doboru narzędzi do różnych scenariuszy.

Kali Linux i popularne narzędzia pentesterskie

Ćwiczenie pracy w Kali Linux oraz praktyczne użycie narzędzi (Nmap, Metasploit, Burp Suite i in.).

Skrypty i automatyzacja ataków

Tworzenie i wykorzystanie skryptów oraz automatyzacja powtarzalnych zadań testowych.

Testy sieciowe i skanowanie

Przeprowadzanie rozpoznania sieciowego, identyfikacja topologii i słabości infrastruktury.

Identyfikacja celów

Mapowanie i selekcja celów oraz priorytetyzacja zasobów do testów.

Skanowanie portów i usług

Wykonywanie skanów portów i usług, interpretacja wyników oraz klasyfikacja zagrożeń.

Analiza podatności

Uruchamianie skanerów podatności, weryfikacja fałszywych trafień i ocena ryzyka.

Eksploatacja systemów

Praktyczne testy eksploatacji znalezionych słabości w kontrolowanym środowisku.

Przełamywanie zabezpieczeń systemów operacyjnych

Wykrywanie i wykorzystywanie słabości OS (Windows/Linux) do uzyskania dostępu.

Wykorzystanie luk w aplikacjach

Testowanie aplikacji pod kątem błędów logicznych i technicznych prowadzących do kompromitacji.

Techniki eskalacji uprawnień

Identyfikacja ścieżek eskalacji i praktyczne metody podnoszenia uprawnień na systemach.

Ataki na aplikacje webowe

Wykrywanie i eksploatacja typowych wektorów ataku w aplikacjach internetowych.

SQL Injection, XSS, CSRF

Ćwiczenie konkretnych technik ataku (SQLi, XSS, CSRF) oraz metod ich wykrywania i mitigacji.

Testowanie logiki biznesowej

Analiza przepływów biznesowych aplikacji w celu wykrycia błędów logicznych i nadużyć.

Testy i ataki na sieci bezprzewodowe

Ocena bezpieczeństwa sieci Wi-Fi i infrastruktury bezprzewodowej.

Ataki na Wi-Fi i sieci korporacyjne

Praktyczne techniki przejęcia dostępu do sieci bezprzewodowych i ich zabezpieczeń.

Post-exploitation i utrzymanie dostępu

Zbieranie danych po uzyskaniu dostępu, tworzenie trwałych kanałów i minimalizowanie śladów.

Zbieranie danych i analiza

Gromadzenie dowodów, logów i artefaktów oraz analiza wpływu na bezpieczeństwo organizacji.

Tworzenie backdoorów i pivoting

Projektowanie kontrolowanych backdoorów oraz pivotowanie w sieci w celu rozszerzenia zasięgu testów.

Raportowanie i dokumentacja

Opracowanie struktury raportu, dokumentowanie odkryć i dowodów w czytelny sposób.

Tworzenie profesjonalnych raportów z testów penetracyjnych

Sporządzanie rekomendacji naprawczych, oceny ryzyka i planu działań korygujących dla klienta.

Szkolenie przygotowuje do certyfikacji OSCP+.

Egzamin OSCP+ Exam

- - egzamin praktyczny na poziomie zaawansowanym, wymagający od uczestnika zastosowania zdobytej wiedzy w realistycznych scenariuszach.

Egzamin OSCP+ jest jednym z najbardziej wymagających certyfikatów pentesterskich, który potwierdza zdolność do przeprowadzania pełnych testów penetracyjnych w realistycznych warunkach.

Cennik

Jeżeli korzystasz z dofinansowania i usługa stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego wraz z usługą lub dostawą towarów ściśle związaną z usługami kształcenia zawodowego lub przekwalifikowania zawodowego to możesz mieć możliwość skorzystania za zwolnienia z podatku VAT na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2024 r. o podatku od towarów i usług, jeśli usługa w całości jest finansowana ze środków publicznych lub § 3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień w przypadku, gdy usługa jest finansowana w co najmniej 70% ze środków publicznych.

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	7 870,77 PLN
Koszt przypadający na 1 uczestnika netto	6 399,00 PLN
Koszt osobogodziny brutto	24,52 PLN
Koszt osobogodziny netto	19,93 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	321:00

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

- **90 dni** dostępu do kursu (materiały do pobrania w pdf. oraz materiały video) i laboratoriów praktycznych **na platformie OffSec**
- Jedno podejście do egzaminu certyfikacyjnego wliczone w cenę.
- Ponad 50 laboratoriów Proving Grounds Play – symulacje ataków w realistycznym środowisku.

Warunki uczestnictwa

Wymagana znajomość języka angielskiego na poziomie B1/B2 (średnio-zaawansowany)

Przed przystąpieniem do kursu zalecamy zdobycie praktycznej wiedzy na temat:

Podstaw sieci TCP/IP

- Adresowanie TCP/IP i podział na podsieci: Cisco — Adresowanie IP i podział na podsieci dla nowych użytkowników
- Protokoły i usługi korzystające z protokołu TCP/IP: Rejestr nazw usług i numerów portów protokołu transportowego
- Sposób dostarczania i odbierania ruchu

Systemów operacyjnych

- Doświadczenie w administracji systemami Windows i Linux: Podróż po systemie Linux, Kali Linux Revealed
- Active Directory: Przegląd usług domenowych Microsoft Active Directory

Języków programowania/skryptowych

- Bash
- Python

Warunki techniczne

Realizacja za pomocą platformy e-learningowej OffSec https://portal.offsec.com

Wymagania sprzętowe:

- komputer z dostępem do internetu o minimalnej przepustowości 20Mb/s.

- wbudowane lub peryferyjne urządzenia do obsługi audio - słuchawki/głośniki oraz mikrofon.

- zainstalowana przeglądarka internetowa - Microsoft Edge/ Internet Explorer 10+ / **Google Chrome** 39+ (sugerowana) / Safari 7+

Kontakt

Ewa Kasprzak

E-mail ewa.kasprzak@softronic.pl

Telefon (+48) 618 658 840