Możliwość dofinansowania

OffSec PEN-200 Penetration Testing with Kali Linux

Numer usługi 2025/06/27/10100/2842039

14 000,00 PLN brutto
14 000,00 PLN netto
400,00 PLN brutto/h
400,00 PLN netto/h

Compendium - Centrum Edukacyjne Spółka z o.o.

4,3 / 5

182 oceny

zdalna w czasie rzeczywistym
Usługa szkoleniowa
35 h
08.09.2025 do 12.09.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Profesjonaliści ds. bezpieczeństwa informacji przechodzący do testów penetracyjnych Pentesterzy poszukujący jednego z najlepszych certyfikatów z zakresu testów penetracyjnych Osoby zainteresowane ścieżką kariery testera penetracyjnego Profesjonaliści ds. bezpieczeństwa Administratorzy sieci Inni specjaliści ds. technologii
Minimalna liczba uczestników	4
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	07-09-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	35
Podstawa uzyskania wpisu do BUR	Znak Jakości Małopolskich Standardów Usług Edukacyjno-Szkoleniowych (MSUES) - wersja 2.0

Cel

Cel edukacyjny

Zwiększ gotowość OSCP dzięki OffSec Academy, sesjom streamingowym prowadzonym przez ekspertów
Dostęp do niedawno wycofanych maszyn egzaminacyjnych OSCP
Wprowadzenie do najnowszych narzędzi i technik hakerskich
Szkolenie prowadzone przez ekspertów Kali Linux
Rozwijaj nastawienie adwersarskie

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Realizacja i zrozumienie zadań testera penetracyjnego	Wykorzystuje techniki gromadzenia informacji w celu identyfikacji i enumeracji celów obsługujących różne systemy operacyjne i usługi.	Wywiad swobodny
Wykorzystuje napisane przez siebie skrypty i narzędzia w procesie testów penetracyjnych	Pisze podstawowe skrypty i narzędzia wspomagające proces testowania penetracyjnego	Wywiad swobodny
Przeprowadzi zdalne, lokalne eskalacje uprawnień i ataków po stronie klienta	Rozumienie i posługuje się testami eskalacji uprawnień i ataków	Wywiad swobodny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

TAK

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Wprowadzenie do cyberbezpieczeństwa

Skuteczne strategie uczenia się

Pisanie raportów dla testerów penetracyjnych

Zbieranie informacji

Skanowanie luk w zabezpieczeniach

Wprowadzenie do aplikacji internetowych

Typowe ataki na aplikacje internetowe

Ataki typu SQL Injection

Ataki po stronie klienta

Lokalizacje publicznych exploitów

Naprawianie exploitów

Unikanie zabezpieczeń antywirusowych

Ataki z użyciem haseł

Eskalacja uprawnień systemu Windows

Eskalacja uprawnień systemu Linux

Przekierowanie portów i tunelowanie SSH

Zaawansowane tunelowanie

Struktura Metasploit

Wprowadzenie i wyliczanie usługi Active Directory

Atakowanie uwierzytelniania usługi Active Directory

Przemieszczanie poziome w usłudze Active Directory

Składanie elementów

Próbując bardziej: laboratoria

Harmonogram

Liczba przedmiotów/zajęć: 0

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	14 000,00 PLN
Koszt przypadający na 1 uczestnika netto	14 000,00 PLN
Koszt osobogodziny brutto	400,00 PLN
Koszt osobogodziny netto	400,00 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnik otrzymuje Autoryzowane materiały szkoleniowe.

Warunki techniczne

Szkolenie obywa się za pośrednictwem platformy **Microsoft Teams.**

Uczestnik może zadawać pytania i aktywnie uczestniczyć w dyskusji. Uczestnik, który potwierdzi swój udział w szkoleniu, przed rozpoczęciem szkolenia, drogą mailową, otrzyma link do spotkania wraz z hasłami dostępu.

Wymagania sprzętowe:

- komputer z dostępem do internetu o minimalnej przepustowości 10Mb/s.

- urządzenie do obsługi audio - słuchawki/glosniki oraz mikrofon.

- zainstalowana dowolna przeglądarka internetowa - np. **Google Chrome**

Kontakt

Michał Dobrzański

E-mail michal.dobrzanski@compendium.pl
Telefon (+48) 122 984 778