Możliwość dofinansowania

FIRMA HANDLOWO - USŁUGOWA ŁUKASZ SOBAŃSKI

Brak ocen dla tego dostawcy

Junior Pentester – pierwsze testy penetracyjne z Kali Linux i Burp Suite. Przygotowanie do pracy w Cyberbezpieczeństwie, przygotowanie do OSCP.

Numer usługi 2026/09/03/236304/3786626

- Usługa szkoleniowa
- zdalna w czasie rzeczywistym
- Zajęcia grupowe
- 16:00 h
- 11.12.2026 do 12.12.2026

3 936,00 PLN	brutto
3 200,00 PLN	netto
246,00 PLN	brutto/h
200,00 PLN	netto/h
261,33 PLN	cena rynkowa

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Usługa szkoleniowa skierowana jest do osób dorosłych zainteresowanych podnoszeniem kompetencji w zakresie cyberbezpieczeństwa i testów penetracyjnych, w szczególności do osób, które chcą poznać podstawy pracy pentestera oraz praktyczne wykorzystanie narzędzi Kali Linux i Burp Suite. W szczególności szkolenie adresowane jest do: • osób rozpoczynających naukę cyberbezpieczeństwa i testów penetracyjnych, • osób planujących rozpoczęcie lub zmianę ścieżki zawodowej w kierunku cyberbezpieczeństwa lub pentestingu, • pracowników branży IT chcących poszerzyć swoje kompetencje o zagadnienia związane z bezpieczeństwem, • osób uczących się samodzielnie cyberbezpieczeństwa i chcących uporządkować oraz rozwinąć swoją wiedzę, • wszystkich osób zainteresowanych poznaniem praktycznych podstaw wykonywania testów bezpieczeństwa aplikacji i systemów. Szkolenie ma charakter podstawowy i jest dostępne również dla osób, które wcześniej nie pracowały w branży IT.
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	10-12-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym

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

Usługa przygotowuje uczestnika do rozpoczęcia dalszej praktycznej nauki testów penetracyjnych poprzez zapoznanie go z procesem realizacji pentestu, podstawowym warsztatem junior pentestera oraz sposobami wykorzystania Kali Linux, Nmap i Burp Suite podczas podstawowej analizy bezpieczeństwa infrastruktury i aplikacji webowych.

Po zakończeniu szkolenia uczestnik będzie przygotowany do rozpoznawania etapów podstawowego testu penetracyjnego i zasad określania jego zakresu, doboru podstawowych narzę

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Identyfikuje podstawowe zasady i etapy realizacji testu penetracyjnego.	Rozpoznaje prawidłową kolejność podstawowych etapów pentestu, zasady określania zakresu testów oraz podstawowe elementy dokumentowania wyników i podatności.	Test teoretyczny z wynikiem generowanym automatycznie
Rozróżnia zastosowanie podstawowych narzędzi wykorzystywanych podczas testów penetracyjnych.	Dobiera Kali Linux, Nmap, WhatWeb, FFUF i Burp Suite do przedstawionych zadań oraz interpretuje podstawowe wyniki rekonesansu i enumeracji.	Test teoretyczny z wynikiem generowanym automatycznie
Analizuje podstawowe elementy komunikacji HTTP oraz sposób wykorzystania Burp Suite podczas testów aplikacji webowych.	Rozpoznaje elementy request/response oraz przyporządkowuje funkcje Proxy, HTTP History, Intercept, Repeater i Intruder do odpowiednich zastosowań w przedstawionym scenariuszu testowym.	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

Dzień 1 – Praca pentestera, Kali Linux i podstawy rekonesansu

Moduł 1. Jak wygląda praca pentestera

- czym jest test penetracyjny i czym różni się od automatycznego skanowania podatności,
- rodzaje testowanych środowisk: aplikacje webowe, infrastruktura, API, systemy wewnętrzne,
- przebieg projektu pentestowego: ustalenie zakresu, zgoda, dostęp, testy, identyfikacja podatności, raport, poprawki i retest,
- pojęcia in scope i out of scope,
- adresy IP, domeny, endpointy, niedozwolone techniki i ograniczenia bezpieczeństwa,
- black box, grey box i white box,
- analiza przykładowego zakresu testu.

Moduł 2. Warsztat Junior Pentestera

- Kali Linux,
- terminal i przeglądarka,
- Burp Suite,
- organizacja notatek,
- lista celów,
- dokumentowanie wyników pentestu.

Moduł 3. Kali Linux – podstawy potrzebne pentesterowi

- terminal, użytkownik, sudo,
- podstawowa struktura katalogów,
- historia poleceń i autouzupełnianie,
- podstawowe polecenia: pwd, ls, cd, cat, grep, find, ip a, ping, curl, wget,
- odczytywanie i zapisywanie wyników podstawowych poleceń.

Moduł 4. Sieć z perspektywy pentestera

- adres IP, host i port,
- TCP i UDP,
- usługa sieciowa,
- klient i serwer,
- DNS,
- HTTP i HTTPS.

Moduł 5. Nmap – pierwsza enumeracja celu

- podstawowy skan,
- skanowanie wybranych portów,
- identyfikacja usług i ich wersji,
- podstawowy skan TCP,
- zapis wyniku,
- interpretacja stanu portów i rozpoznanych usług,
- różnica pomiędzy otwartym portem a podatnością.

Moduł 6. Rekonesans aplikacji webowej

- podstawowe zastosowanie WhatWeb,
- podstawowe informacje DNS,
- idea content discovery,
- podstawowe użycie FFUF,
- wordlisty,
- interpretacja kodów 200, 301/302 i 403,
- false positives.

Moduł 7. HTTP – fundament pentestów webowych

- request i response,
- GET i POST,
- URL i endpoint,
- parametry,
- nagłówki,
- cookies,
- body,
- kody odpowiedzi HTTP.

Dzień 2 – Burp Suite i podstawowy workflow pentestu webowego

Moduł 8. Burp Suite – przygotowanie i podstawy

- przygotowanie narzędzia do pracy,
- omówienie podstawowych elementów interfejsu,
- rola Burp Suite w analizie ruchu aplikacji webowej.

Moduł 9. Proxy i HTTP History

- obserwowanie ruchu pomiędzy przeglądarką i aplikacją,
- analiza zarejestrowanych żądań i odpowiedzi,
- wybór interesujących requestów do dalszej analizy.

Moduł 10. Intercept i Repeater

- Intercept On/Off,
- zatrzymanie żądania,
- modyfikacja parametru,
- Forward i Drop,
- Send to Repeater,
- modyfikowanie i wielokrotne wysyłanie żądania,
- analiza odpowiedzi aplikacji.

Moduł 11. Scope w Burp Suite

- Target,
- Scope,
- Include i Exclude,
- filtrowanie ruchu do celów znajdujących się w zakresie testów.

Moduł 12. Intruder – podstawowa automatyzacja

- wskazanie pozycji w żądaniu,
- payload,
- prosta lista wartości,
- uruchomienie ataku testowego,
- analiza kodów i długości odpowiedzi,
- różnica pomiędzy ręcznym testowaniem w Repeater a automatyzacją w Intruder.

Moduł 13. Demonstracyjny mini-pentest aplikacji

- ustalenie celu i Scope,
- przegląd aplikacji,
- analiza HTTP History,

- wybór żądania,
- przekazanie go do Repeatera,
- modyfikacja parametru,
- analiza odpowiedzi,
- potwierdzenie nieprawidłowego zachowania,
- wykonanie materiału dowodowego i zapis request/response.

Moduł 14. Dokumentowanie podatności i podstawy raportowania

- tytuł podatności,
- opis,
- request i response,
- kroki reprodukcji,
- PoC,
- zagrożenie,
- rekomendacja,
- severity,
- raport techniczny,
- executive summary,
- retest

Usługa prowadzi do nabycia kompetencji cyfrowych w rozumieniu Europejskiej Ramy Kompetencji Cyfrowych DigComp, w szczególności w obszarze 4. Bezpieczeństwo oraz 5. Rozwiązywanie problemów.

Harmonogram

Liczba pozycji harmonogramu: 21

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 21 Jak wygląda praca pentestera (współdzielenie ekranu, czat, dyskusja moderowana, pokoje Zoom)	Zajęcia	ŁUKASZ SOBAŃSKI	11-12-2026	09:00	10:00	01:00
2 z 21 Warsztat Junior Pentestera (współdzielenie ekranu, czat, dyskusja moderowana, pokoje Zoom)	Zajęcia	ŁUKASZ SOBAŃSKI	11-12-2026	10:00	10:45	00:45
3 z 21 -	Przerwa	-	11-12-2026	10:45	11:00	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
4 z 21 Kali Linux – podstawy potrzebne pentesterowi (współdzielenie ekranu, czat, dyskusja moderowana, pokoje Zoom)	Zajęcia	ŁUKASZ SOBAŃSKI	11-12-2026	11:00	12:00	01:00
5 z 21 Sieć z perspektywy pentestera (współdzielenie ekranu, czat, dyskusja moderowana, pokoje Zoom)	Zajęcia	ŁUKASZ SOBAŃSKI	11-12-2026	12:00	12:45	00:45
6 z 21 -	Przerwa	-	11-12-2026	12:45	13:15	00:30
7 z 21 Nmap – pierwsza enumeracja celu (współdzielenie ekranu, czat, dyskusja moderowana, pokoje Zoom)	Zajęcia	ŁUKASZ SOBAŃSKI	11-12-2026	13:15	14:30	01:15
8 z 21 -	Przerwa	-	11-12-2026	14:30	14:45	00:15
9 z 21 Rekonesans aplikacji webowej (współdzielenie ekranu, czat, dyskusja moderowana, pokoje Zoom)	Zajęcia	ŁUKASZ SOBAŃSKI	11-12-2026	14:45	16:00	01:15
10 z 21 HTTP – fundament pentestów webowych (współdzielenie ekranu, czat, dyskusja moderowana, pokoje Zoom)	Zajęcia	ŁUKASZ SOBAŃSKI	11-12-2026	16:00	17:00	01:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
11 z 21 Burp Suite – przygotowanie i podstawy (współdzielenie ekranu, czat, dyskusja moderowana, pokoje Zoom)	Zajęcia	ŁUKASZ SOBAŃSKI	12-12-2026	09:00	10:00	01:00
12 z 21 Proxy i HTTP History (współdzielenie ekranu, czat, dyskusja moderowana, pokoje Zoom)	Zajęcia	ŁUKASZ SOBAŃSKI	12-12-2026	10:00	10:45	00:45
13 z 21 -	Przerwa	-	12-12-2026	10:45	11:00	00:15
14 z 21 Intercept i Repeater (współdzielenie ekranu, czat, dyskusja moderowana, pokoje Zoom)	Zajęcia	ŁUKASZ SOBAŃSKI	12-12-2026	11:00	12:15	01:15
15 z 21 Scope w Burp Suite (współdzielenie ekranu, czat, dyskusja moderowana, pokoje Zoom)	Zajęcia	ŁUKASZ SOBAŃSKI	12-12-2026	12:15	12:45	00:30
16 z 21 -	Przerwa	-	12-12-2026	12:45	13:15	00:30
17 z 21 Intruder – podstawowa automatyzacja (współdzielenie ekranu, czat, dyskusja moderowana, pokoje Zoom)	Zajęcia	ŁUKASZ SOBAŃSKI	12-12-2026	13:15	14:30	01:15
18 z 21 -	Przerwa	-	12-12-2026	14:30	14:45	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
19 z 21 Demonstracyjny mini-pentest aplikacji (współdzielenie ekranu, czat, dyskusja moderowana, pokoje Zoom)	Zajęcia	ŁUKASZ SOBAŃSKI	12-12-2026	14:45	15:45	01:00
20 z 21 Dokumentowanie podatności i podstawy raportowania (współdzielenie ekranu, czat, dyskusja moderowana, pokoje Zoom)	Zajęcia	ŁUKASZ SOBAŃSKI	12-12-2026	15:45	16:30	00:45
21 z 21 -	Walidacja	ŁUKASZ SOBAŃSKI	12-12-2026	16:30	17:00	00:30

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	16:00
w tym suma godzin zajęć	13:30
w tym suma godzin walidacji	00:30
w tym suma przerw	02:00
Suma godzin dydaktycznych bez przerw	18:30

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 2004 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	3 936,00 PLN
Koszt przypadający na 1 uczestnika netto	3 200,00 PLN
Koszt osobogodziny brutto	246,00 PLN
Koszt osobogodziny netto	200,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	16:00

Prowadzący

Liczba prowadzących: 1

1 z 1

ŁUKASZ SOBAŃSKI

Specjalista ds. cyberbezpieczeństwa posiadający ponad 5 letnie doświadczenie zawodowe w realizacji audytów bezpieczeństwa, testów penetracyjnych aplikacji webowych oraz ocenie bezpieczeństwa środowisk informatycznych. W pracy wykorzystuje m.in. Kali Linux, Burp Suite oraz narzędzia służące do rekonesansu, enumeracji i analizy bezpieczeństwa aplikacji oraz infrastruktury. Posiadacz certyfikatów branżowych m.in. OSWE, OSCP, OSWP, BSCP oraz AZ-500.

- Zweryfikuj OSCP: https://credentials.offsec.com/d966c5fa-e54c-4f94-9ce3-ad13a1c56da6#acc.qQUmypDi
- Zweryfikuj OSWE: https://credentials.offsec.com/18367b6c-58d8-4ab5-833b-0dccff04abd6#acc.VwF0zZOx
- Zweryfikuj OSWP: https://credentials.offsec.com/f6a7c773-d1ff-4fe8-9928-31dd708f555c#acc.KB63pynS
- Zweryfikuj BSCP: https://portswigger.net/web-security/e/c/0c24c66157beff2d

LinkedIn trenera: https://www.linkedin.com/in/lucsobanski/

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy szkolenia otrzymają dostęp do współdzielonego dysku Google, na którym udostępnione zostaną materiały wykorzystywane przez prowadzącego podczas realizacji szkolenia.

Materiały obejmują w szczególności:

- skrypty i przykładowe pliki wykorzystywane podczas prezentowanych ćwiczeń,
- pliki konfiguracyjne i pomocnicze,
- zestawy poleceń prezentowanych podczas szkolenia,
- dodatkowe materiały wspierające samodzielne utrwalenie zdobytej wiedzy.

Dostęp do materiałów zostanie przekazany uczestnikom w formie elektronicznej.

Warunki uczestnictwa

Szkolenie przeznaczone jest dla osób początkujących i nie wymaga wcześniejszego doświadczenia w testach penetracyjnych. Wymagana jest podstawowa umiejętność obsługi komputera oraz korzystania ze stron internetowych.

Uczestnik musi posiadać komputer lub laptop z dostępem do Internetu, aktualną przeglądarkę internetową oraz możliwość udziału w spotkaniu online.

Opcjonalnie uczestnik może przygotować własne środowisko Kali Linux oraz Burp Suite Community w celu równoległego odtwarzania działań prezentowanych przez trenera. Posiadanie tych narzędzi nie jest wymagane do udziału w szkoleniu ani do przeprowadzenia walidacji.

Wymagania organizacyjne

- uczestnik zobowiązany jest do logowania się na zajęcia w wyznaczonych terminach,
- udział w szkoleniu online wymaga aktywnego uczestnictwa, w tym możliwości zadawania pytań oraz udziału w dyskusjach,
- materiały dydaktyczne udostępniane są w formie elektronicznej.

Informacje dodatkowe

Szkolenie ma charakter demonstracyjno-warsztatowy. Trener udostępnia własny ekran i prezentuje działania w przygotowanych środowiskach laboratoryjnych. Uczestnicy mogą równolegle odtwarzać prezentowane czynności we własnym środowisku, jednak ich działania nie są indywidualnie obserwowane ani oceniane przez trenera. Formalna walidacja efektów uczenia się odbywa się wyłącznie za pomocą testu teoretycznego online z wynikiem generowanym automatycznie.

Informacja dotycząca podatku VAT:

Podstawa zwolnienia z podatku VAT:

- § 3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. – w przypadku dofinansowania usługi w wysokości co najmniej 70%.

W przypadku braku dofinansowania lub dofinansowania poniżej 70%, do ceny usługi doliczany jest podatek VAT w wysokości 23%.

Warunki techniczne

Usługa realizowana jest zdalnie w czasie rzeczywistym za pośrednictwem platformy Zoom [lub innej wskazanej przez Dostawcę platformy komunikacyjnej].

Minimalne wymagania techniczne po stronie uczestnika:

- komputer lub laptop z dostępem do Internetu,

- aktualna wersja przeglądarki internetowej,
- możliwość uruchomienia aplikacji Zoom lub skorzystania z wersji przeglądarkowej,
- mikrofon i kamera internetowa,
- głośniki lub słuchawki,
- stabilne połączenie z Internetem umożliwiające udział w transmisji audio-wideo oraz odbiór współdzielonego ekranu,
- możliwość otwarcia strony internetowej służącej do przeprowadzenia testu walidacyjnego.

Instalacja Kali Linux oraz Burp Suite po stronie uczestnika jest opcjonalna i nie stanowi warunku uczestnictwa w usłudze.

Kontakt

Łukasz Sobański

E-mail kontakt@luxszkolenia.pl

Telefon (+48) 797 463 050