Możliwość dofinansowania

ALTKOM AKADEMIA SPÓŁKA AKCYJNA

★★★★½

Certified Penetration Testing Professional v1 - forma zdalna w czasie rzeczywistym

Numer usługi 2024/09/19/120967/2316639

9 840,00 PLN brutto
8 000,00 PLN netto
153,75 PLN brutto/h
125,00 PLN netto/h

zdalna w czasie rzeczywistym
Usługa szkoleniowa
64 h
12.05.2025 do 13.06.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Szkolenie jest dedykowane wszystkim, którzy chcą stać się ekspertami w dziedzinie testów penetracyjnych i uzyskać dogłębną wiedzę na temat najbardziej zaawansowanych narzędzi, technik i metodologii testowania penetracyjnego.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	05-05-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	64
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Usługa potwierdza przygotowanie Uczestnika do rozróżniania podstawowych pojęć dotyczących testów penetracyjnych, w tym ich znaczenia, rodzajów, procesu, faz i metodologii, a także wiedzy jak wdrożyć kompleksową metodologię testów penetracyjnych. Uczestnik po szkoleniu

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Definiuje podstawowe pojęcia dotyczące testów penetracyjnych, w tym ich znaczenie, rodzaje, proces, fazy i metodologie	- definiuje podstawowe pojęcia dotyczące testów penetracyjnych - definiuje rodzaje testów penetracyjnych - charakteryzuje proces, fazy i metodologie testów penetracyjnych	Test teoretyczny
Inicjuje, angażuje i kontynuuje zadanie testowania penetracyjnego	- charakteryzuje techniki zbierania informacji o celu z różnych publicznie dostępnych źródeł	Test teoretyczny
Wdraża kompleksową metodologię testów penetracyjnych	- charakteryzuje zasady wdrażania kompleksowej metodologii testów penetracyjnych w celu oceny ludzkich zachowań - charakteryzuje zasady wdrażania kompleksowej metodologii testów penetracyjnych do oceny sieci z perspektywy osób postronnych - charakteryzuje zasady wdrażania kompleksowej metodologii testów penetracyjnych do oceny sieci z perspektywy osób postronnych - charakteryzuje zasady wdrażania kompleksowej metodologii testów penetracyjnych do oceny bezpieczeństwa sieciowych urządzeń perymetrycznych - charakteryzuje zasady wdrażania kompleksowej metodologii testów penetracyjnych do oceny bezpieczeństwa aplikacji internetowych i serwerów internetowych organizacji	Test teoretyczny
Ustanawia proces oceny urządzeń IoT	- charakteryzuje zasady wyodrębniania oprogramowania układowego z urządzeń - charakteryzuje zasady montowania i uruchamiania obrazu oprogramowania układowego - charakteryzuje zasady badania exploitów IoT	Test teoretyczny
Pisze kompleksowy raport z testów penetracyjnych dla docelowych odbiorców	- charakteryzuje zasady pisania kompleksowego raportu z testów penetracyjnych dla docelowych odbiorców	Test teoretyczny

Kwalifikacje

Inne kwalifikacje

Uznane kwalifikacje

Pytanie 5. Czy dokument jest certyfikatem, dla którego wypracowano system walidacji i certyfikowania efektów uczenia się na poziomie międzynarodowym?

tak

Informacje

Podstawa prawna dla Podmiotów / kategorii Podmiotów	uprawnione do realizacji procesów walidacji i certyfikowania na mocy innych przepisów prawa
Nazwa/Kategoria Podmiotu prowadzącego walidację	EC-Council
Podmiot prowadzący walidację jest zarejestrowany w BUR	Nie
Nazwa/Kategoria Podmiotu certyfikującego	EC-Council
Podmiot certyfikujący jest zarejestrowany w BUR	Nie

Program

Agenda szkolenia:

1. Wprowadzenie do testów penetracyjnych
2. Zakres testów penetracyjnych
3. Open Source Intelligence (OSINT)
4. Testy penetracyjne – inżynieria społeczna
5. Testy penetracyjne sieci – zewnętrzne
6. Testy penetracyjne sieci – wewnętrzne
7. Testy penetracyjne sieci – urządzenia obwodowe
8. Testy penetracyjne aplikacji internetowych
9. Testy penetracyjne – sieć bezprzewodowa
10. Testy penetracyjne IoT
11. Testy penetracyjne OT/SCADA
12. Testy penetracyjne – chmura
13. Analiza binarna
14. Pisanie raportów i działania po testach
15. Egzamin

Przerwy wliczają się w czas szkolenia.

Szkolenie realizowane w godzinach zegarowych.

Metoda egzaminowania:

Po zakończonym szkoleniu Uczestnik otrzymuje voucher na egzamin do wykorzystania do ostatniego dnia usługi.

CPENT jest egzaminem praktycznym w całości przeprowadzanym zdalnie w języku angielskim. Egzamin jest przez przeprowadzany w obecności osoby pełniącej role nadzorcy. Osoba przystępująca do egzaminu przez cały czas trwania egzaminu musi posiadać włączoną kamerę, mikrofon i udostępniony ekran.

Egzamin można zdawać w formie jednej sesji 24 godzinnej lub dwóch sesjach po 12 godzin każda.

Egzamin wpisany w harmonogram na prawdopodobny termin i godziny.

Certyfikat CPENT otrzymują kandydaci, którzy uzyskali 70% możliwych do uzyskania punktów, certyfikat LPT wymaga uzyskania co najmniej 90%.

Kandydaci, którzy uzyskają wynik powyżej 90%, zostaną uznani jako Penetration Testing Masters i zdobędą prestiżowy certyfikat LPT(Master).

Wymagania ogólne realizacji szkolenia w formule distance learning (online): Komputer stacjonarny lub notebook wyposażony w mikrofon, głośniki i kamerę internetową z przeglądarką internetową z obsługą HTML 5. Monitor o rozdzielczości FullHD. Szerokopasmowy dostęp do Internetu o przepustowości co najmniej 25/5 (download/upload) Mb/s. W przypadku szkoleń z laboratoriami zalecamy: sprzęt wyposażony w dwa ekrany o rozdzielczości minimum HD (lub dwa komputery), kamerę internetową USB, zewnętrzne głośniki lub słuchawki.

Platforma komunikacji – ZOOM

Oprogramowanie – zdalny pulpit, aplikacja ZOOM

Link do szkolenia zgodnie z regulaminem zostanie wysłany na 2 dni przed rozpoczęciem usługi.

Link do szkolenia jest ważny w trakcie trwania całej usługi szkoleniowej.

Harmonogram

Liczba przedmiotów/zajęć: 22

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 22 Wprowadzenie do testów penetracyjnych wykład	Kamil Malinowski	12-05-2025	10:00	11:00	01:00
2 z 22 Zakres testów penetracyjnych ćwiczenia	Kamil Malinowski	12-05-2025	11:00	13:00	02:00
3 z 22 Przerwa	Kamil Malinowski	12-05-2025	13:00	13:15	00:15
4 z 22 Open Source Intelligence (OSINT) cz. 1 ćwiczenia	Kamil Malinowski	12-05-2025	13:15	18:00	04:45

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 22 Open Source Intelligence (OSINT) cz.2 ćwiczenia	Kamil Malinowski	13-05-2025	09:00	11:00	02:00
6 z 22 Testy penetracyjne – inżynieria społeczna ćwiczenia	Kamil Malinowski	13-05-2025	11:00	13:00	02:00
7 z 22 Przerwa	Kamil Malinowski	13-05-2025	13:00	13:15	00:15
8 z 22 Testy penetracyjne sieci – zewnętrzne ćwiczenia	Kamil Malinowski	13-05-2025	13:15	17:00	03:45
9 z 22 Testy penetracyjne sieci – wewnętrzne ćwiczenia	Kamil Malinowski	14-05-2025	09:00	11:00	02:00
10 z 22 Testy penetracyjne sieci – urządzenia obwodowe ćwiczenia	Kamil Malinowski	14-05-2025	11:00	13:00	02:00
11 z 22 Przerwa	Kamil Malinowski	14-05-2025	13:00	13:15	00:15
12 z 22 Testy penetracyjne aplikacji internetowych ćwiczenia	Kamil Malinowski	14-05-2025	13:15	17:00	03:45
13 z 22 Testy penetracyjne – sieć bezprzewodowa ćwiczenia	Kamil Malinowski	15-05-2025	09:00	11:00	02:00
14 z 22 Testy penetracyjne IoT ćwiczenia	Kamil Malinowski	15-05-2025	11:00	13:00	02:00
15 z 22 Przerwa	Kamil Malinowski	15-05-2025	13:00	13:15	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
16 z 22 Testy penetracyjne OT/SCADA ćwiczenia	Kamil Malinowski	15-05-2025	13:15	17:00	03:45
17 z 22 Testy penetracyjne – chmura ćwiczenia	Kamil Malinowski	16-05-2025	09:00	11:00	02:00
18 z 22 Analiza binarna ćwiczenia	Kamil Malinowski	16-05-2025	11:00	13:00	02:00
19 z 22 Przerwa	Kamil Malinowski	16-05-2025	13:00	13:15	00:15
20 z 22 Pisanie raportów i działania po testach ćwiczenia	Kamil Malinowski	16-05-2025	13:15	17:00	03:45
21 z 22 Egzamin cz.1	-	12-06-2025	07:00	19:00	12:00
22 z 22 Egzamin cz.2	-	13-06-2025	07:00	19:00	12:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	9 840,00 PLN
Koszt przypadający na 1 uczestnika netto	8 000,00 PLN
Koszt osobogodziny brutto	153,75 PLN
Koszt osobogodziny netto	125,00 PLN
W tym koszt walidacji brutto	4 920,00 PLN
W tym koszt walidacji netto	4 000,00 PLN

W tym koszt certyfikowania brutto	1,23 PLN
W tym koszt certyfikowania netto	1,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Kamil Malinowski

Wykształcenie: Uniwersytet w Białymstoku
Studia I-go stopnia na Wydziale Matematyki i Informatyki
• Politechnika Białostocka
Studia II-go stopnia na Wydziale Informatyki
• Szkoła Doktorska Politechniki Białostockiej
Studia III-go stopnia
Specjalizacja: Bezpieczeństwo IT
• Wirtualizacja
• Systemy serwerowe.
Doświadczenie trenerskie: Obecnie trener Altkom Akademii. Posiada ponad 16 lat doświadczenia w branży IT. Posiada doświadczenie trenerskie zdobyte w ciągu ostatnich 5 lat. Pracował jako ekspert projektując i wdrażając całe infrastruktury dla wielu firm, urzędów i instytucji. Odpowiadał za prowadzenie złożonych projektów związanych z warstwą serwerowostorage'ową, wirtualizacją, bezpieczeństwem systemowym i sieciowym.
ZAKRES TEMATYCZNY PROWADZONYCH SZKOLEŃ:
• Wprowadzenie do zagadnień bezpieczeństwa IT – BS.IT 01
• Warsztaty z wybranych elementów bezpieczeństwa IT – BS.IT 02
• EC-COUNCIL CPENT

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Na platformie Wirtualna Klasa Altkom Akademii udostępnione zostaną bezterminowo materiały szkoleniowe (tj. np. podręczniki/prezentacje/materiały dydaktyczne niezbędne do odbycia szkolenia/ebooki itp.), zasoby bazy wiedzy portalu oraz dodatkowe informacje od trenera. Uczestnicy zachowują bezterminowy dostęp do zasobów Mojej Akademii i materiałów szkoleniowych zgromadzonych w Wirtualnej Klasie szkolenia. Platforma do kontaktu z trenerami, grupą i całą społecznością absolwentów jest portal Moja Akademia.

Warunki uczestnictwa

Niezbędnym warunkiem uczestnictwa w szkoleniach dofinansowanych z funduszy europejskich jest założenie konta w Bazie Usług Rozwojowych, zapis na szkolenie za pośrednictwem Bazy oraz spełnienie warunków przedstawionych przez danego Operatora, dysponenta funduszy publicznych, do którego składają Państwo dokumenty o dofinansowanie do usługi rozwojowej.

Ogólne warunki uczestnictwa w zajęciach zostały zamieszczone na stronie: https://www.altkomakademia.pl/ogolne-warunki-uczestnictwa-w-szkoleniach/

Informacje dodatkowe

Po szkoleniu Uczestnik otrzyma zaświadczenie o ukończeniu szkolenia.

Trener podczas szkolenia będzie organizował krótkie przerwy. Informacja o przerwach będzie umieszczona na slajdzie.

Warunki techniczne

Wymagania ogólne realizacji szkolenia w formule distance learning (online): Komputer stacjonarny lub notebook wyposażony w mikrofon, głośniki i kamerę internetową z przeglądarką internetową z obsługą HTML 5. Monitor o rozdzielczości FullHD. Szerokopasmowy dostęp do Internetu o przepustowości co najmniej 25/5 (download/upload) Mb/s. W przypadku szkoleń z laboratoriami zalecamy: sprzęt wyposażony w dwa ekrany o rozdzielczości minimum HD (lub dwa komputery), kamerę internetową USB, zewnętrzne głośniki lub słuchawki.

Platforma komunikacji – ZOOM

Oprogramowanie – zdalny pulpit, aplikacja ZOOM

Link do szkolenia zgodnie z regulaminem zostanie wysłany na 2 dni przed rozpoczęciem usługi.

Link do szkolenia jest ważny w trakcie trwania całej usługi szkoleniowej.

Kontakt

Agnieszka Sipura

E-mail agnieszka.sipura@altkom.pl
Telefon (+48) 609 191 281