Możliwość dofinansowania

Szkolenie C PenTest+ CompTIA PenTest+

Numer usługi 2024/05/22/142469/2158345

5 535,00 PLN brutto
4 500,00 PLN netto
158,14 PLN brutto/h
128,57 PLN netto/h

SOFTRONIC SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

★★★★½

zdalna w czasie rzeczywistym
Usługa szkoleniowa
35 h
16.09.2024 do 20.09.2024

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Szkolenie **CompTIA PenTest+** jest skierowane do profesjonalistów ds. bezpieczeństwa informatycznego, testerów penetracyjnych oraz analityków bezpieczeństwa, którzy zajmują się identyfikacją i zwalczaniem zagrożeń cybernetycznych. Grupa docelowa obejmuje osoby z zaawansowaną wiedzą i doświadczeniem w dziedzinie testów penetracyjnych, które chcą rozwijać umiejętności w zakresie penetracji sieci i aplikacji.
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	7
Data zakończenia rekrutacji	30-08-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	35
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

Szkolenie CompTIA PenTest+ ma na celu dostarczenie zaawansowanej wiedzy i umiejętności testerom penetracyjnym oraz specjalistom ds. bezpieczeństwa informatycznego.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozumie podstawowe koncepcje dotyczące testowania penetracyjnego	definiuje testowanie penetracyjne i jego cele, omawia różnice między testowaniem penetracyjnym a testowaniem bezpieczeństwa, wyjaśnia proces określania zakresu wymagań organizacyjnych/klienta.	Test teoretyczny
Potrafi przeprowadzać footprinting i zbierać informacje	opisuje techniki footprintingu i ich zastosowanie, zbiera informacje o organizacji lub systemie zgodnie z określonymi celami, identyfikuje różne źródła informacji używane podczas footprintingu.	Test teoretyczny
Ocenia ludzkie i fizyczne słabe punkty	rozpoznaje i analizuje ludzkie słabe punkty w kontekście bezpieczeństwa, rozpoznaje i analizuje fizyczne słabe punkty w infrastrukturze organizacyjnej, formułuje rekomendacje dotyczące poprawy zarządzania słabymi punktami.	Test teoretyczny
Potrafi przygotować skanowanie podatności	konfiguruje narzędzia do skanowania podatności, przygotowuje zbiór reguł skanowania podatności logicznych, interpretuje wyniki skanowania i tworzy raporty.	Test teoretyczny
Przeprowadza testy penetracyjne aplikacji internetowych	opisuje techniki ataków na aplikacje internetowe (np. SQL injection, XSS), wykorzystuje narzędzia do automatycznego skanowania i testowania aplikacji webowych, analizuje wyniki testów i formułuje zalecenia dotyczące poprawy bezpieczeństwa aplikacji.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wykorzystuje sieci LAN i chmurę do testowania	konfiguruje sieci LAN do przeprowadzania testów penetracyjnych, wykorzystuje chmurę do symulacji i testowania zewnętrznych ataków, analizuje zalety i wyzwania związane z wykorzystaniem sieci LAN i chmury w testowaniu.	Test teoretyczny
Atakuje urządzenia mobilne	identyfikuje podatności i luki bezpieczeństwa w systemach operacyjnych mobilnych, stosuje techniki testowania penetracyjnego do atakowania urządzeń mobilnych, demonstruje umiejętność ominięcia zabezpieczeń i uzyskania dostępu do danych na urządzeniach mobilnych.	Test teoretyczny
Tworzy skrypty i oprogramowanie do automatyzacji testów	pisze skrypty do automatyzacji procesów testowania penetracyjnego, tworzy narzędzia lub modyfikuje istniejące oprogramowanie do testowania bezpieczeństwa, demonstruje umiejętność analizy i poprawy skryptów oraz narzędzi.	Test teoretyczny
Komunikuje efekty testowania penetracyjnego	przygotowuje raporty z wynikami testów penetracyjnych, prezentuje wyniki testów i rekomendacje klientowi lub decydentom, prowadzi dyskusje na temat zidentyfikowanych zagrożeń i proponowanych środków zaradczych.	Test teoretyczny
Realizuje działania po dostarczeniu raportu	monitoruje i ocenia wdrożenie rekomendacji z raportu, udziela wsparcia przy implementacji zaleceń bezpieczeństwa, przeprowadza ewaluację działań i reaguje na nowe zagrożenia.	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

Tak, Uczestnik szkolenia, poza certyfikatem, otrzymuje zaświadczenie o ukończeniu szkolenia z zawartym opisem efektów uczenia się.

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

Szkolenie **CompTIA PenTest+** skupia się na zaawansowanych umiejętnościach z zakresu testów penetracyjnych. Uczestnicy zdobywają głęboką wiedzę z identyfikacji, oceny i eksploatacji potencjalnych luk w zabezpieczeniach sieci i aplikacji, wykorzystując różnorodne narzędzia i techniki. Program szkoleniowy umożliwia skuteczne przeprowadzanie testów penetracyjnych oraz dostarczanie szczegółowych raportów z zaleceniami bezpieczeństwa. Po ukończeniu szkolenia, absolwenci są przygotowani do roli specjalistów ds. testów penetracyjnych, oferując wartościowy wkład w zabezpieczanie organizacji przed cyberzagrożeniami.

Szkolenie składa się z wykładu wzbogaconego o prezentację. W trakcie szkolenia każdy Uczestnik wykonuje indywidualne ćwiczenia - laboratoria, dzięki czemu zyskuje praktyczne umiejętności. W trakcie szkolenia omawiane jest również studium przypadków, w którym Uczestnicy wspólnie wymieniają się doświadczeniami. Nad case-study czuwa autoryzowany Trener, który przekazuje informację na temat przydatnych narzędzi oraz najlepszych praktyk do rozwiązania omawianego zagadnienia.

Aby Uczestnik osiągnął zamierzony cel szkolenia niezbędne jest wykonanie przez niego zadanych laboratoriów. Pomocne będzie również ugruntowanie wiedzy i wykonywanie ćwiczeń po zakończonej usłudze. Każdy Uczestnik dysponuje dostępem do laboratoriów przez okres 180 dni.

Szkolenie trwa 40godzin zegarowych i jest realizowane w ciągu 5 dni.
W trakcie każdego dnia szkolenia przewidziane są dwie krótkie przerwy "kawowe" oraz przerwa lunchowa.

Program szkolenia

Określanie zakresu wymagań organizacyjnych/klienta

Definiowanie zasad zaangażowania

Footprinting i zbieranie informacji

Ocena ludzkich i fizycznych słabych punktów

Przygotowanie skanowania podatności

Skanowanie podatności logicznych

Analiza wyników skanowania

Unikanie wykrycia i zacieranie śladów

Wykorzystywanie sieci LAN i chmury

Testowanie sieci bezprzewodowych

Ataki na urządzenia mobilne

Atakowanie wyspecjalizowanych systemów

Ataki oparte na aplikacjach internetowych

Przeprowadzanie włamań do systemów

Tworzenie skryptów i oprogramowania

Wykorzystanie ataku: Obrót i penetracja

Komunikacja podczas procesu testowania penetracyjnego

Podsumowanie komponentów raportu

Rekomendowanie środków zaradczych

Wykonywanie działań po dostarczeniu raportu

SOFTRONIC Sp. z o. o. zastrzega sobie prawo do zmiany terminu szkolenia lub jego odwołania w przypadku niezebrania się minimalnej liczby Uczestników tj. 3 osób.

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	5 535,00 PLN
Koszt przypadający na 1 uczestnika netto	4 500,00 PLN
Koszt osobogodziny brutto	158,14 PLN
Koszt osobogodziny netto	128,57 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdemu Uczestnikowi zostaną przekazane autoryzowane materiały szkoleniowe Comptia.

Warunki uczestnictwa

Przed przystąpieniem do szkolenia Uczestnik powinien posiadać podstawową wiedzę z zakresu bezpieczeństwa informatycznego oraz znajomość podstawowych pojęć związanych z sieciami komputerowymi. Doświadczenie w administracji systemami oraz podstawowa znajomość protokołów sieciowych będzie również korzystne.

Informacje dodatkowe

Istnieje możliwość zastosowania zwolnienia z podatku VAT dla szkoleń mających charakter kształcenia zawodowego lub służących przekwalifikowaniu zawodowemu pracowników, których poziom dofinansowania ze środków publicznych wynosi co najmniej 70% (na podstawie § 3 ust. 1 pkt 14 Rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. zmieniające rozporządzenie w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień (Dz. U. z 2013 r. poz. 1722 ze zm.)

Warunki techniczne

Szkolenie realizowane jest w formule distance learning - szkolenie **on-line w czasie rzeczywistym**, w którym możesz wziąć udział z każdego miejsca na świecie.

Szkolenie obywa się za pośrednictwem platformy **Microsoft Teams**, która umożliwia transmisję dwukierunkową, dzięki czemu Uczestnik może zadawać pytania i aktywnie uczestniczyć w dyskusji. Uczestnik, ktory potwierdzi swój udziałw szkoleniu, przed rozpoczęciem szkolenia, drogą mailową, otrzyma link do spotkania wraz z hasłami dostępu.

Wymagania sprzętowe:
- komputer z dostępem do internetu o minimalnej przepustowości 20Mb/s.
- wbudowane lub peryferyjne urządzenia do obsługi audio - słuchawki/glosniki oraz mikrofon.
- zainstalowana przeglądarka internetowa - Microsoft Edge/ Internet Explorer 10+ / **Google Chrome** 39+ (sugerowana) / Safari 7+
- aplikacja MS Teams może zostać zainstalowana na komputerze lub można z niej korzystać za pośrednictwem przeglądarki internetowej

Kontakt

Ewa Kasprzak

E-mail ewa.kasprzak@softronic.pl
Telefon (+48) 618 658 840