Możliwość dofinansowania

Dagma sp. z o.o.

★★★★½

CEH - Certified Ethical Hacker v12

Numer usługi 2024/11/06/17164/2398979

8 474,70 PLN brutto
6 890,00 PLN netto
211,87 PLN brutto/h
172,25 PLN netto/h

zdalna w czasie rzeczywistym
Usługa szkoleniowa
40 h
16.12.2024 do 20.12.2024

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Szkolenie skierowane do pracowników sektora IT, w tym administratorów sieci, osób odpowiedzialnych za infrastrukturę informatyczną, tzw. security officers, audytorów, specjalistów ds. bezpieczeństwa informatycznego, administratorów witryn oraz każdego, kto planuje podniesienie poziomu bezpieczeństwa informatycznego swojej organizacji.
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	09-12-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	40
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 szkolenia jest dostarczenie kompetencji z zakresu CERTIFIED ETHICAL HACKER v12, dzięki którym uczestnik będzie samodzielnie dokonywał kontrolowanych włamań do systemu „ofiary", identyfikował słabe punkty organizacji, skanował, testował i przełamywał zabezpieczenia systemów.
Uczestnik po ukończonym szkoleniu nabędzie kompetencje społeczne takie jak samokształcenie, rozwiązywanie problemów, kreatywność w działaniu.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik posługuje się narzędziami, technikami i metodologiami wykorzystywanymi przez realnych hakerów; efektywnie ochrania sieci.	Samodzielna praca w środowisku wirtualnym	Obserwacja w warunkach symulowanych

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

Moduł 1 Wprowadzenie do „Etycznego Hakingu - zajęcia teoretyczne (wykład)

Moduł 2 Wstępne zbieranie informacji o celu ataku - zajęcia teoretyczne (wykład)

Moduł 3 Skanowanie sieci - identyfikacja systemów, portów, usług działających w sieci - zajęcia praktyczne (ćwiczenia)

- Aktywne odpytywanie usług/systemów w celu rozpoznania słabych punktów w infrastrukturze

Moduł 4 Enumeracja - zajęcia teoretyczne (wykład)

Moduł 5 Analiza podatności - omówienie narzędzi do wykonywania skanowania oraz kryteriów ich doboru - zajęcia teoretyczne (wykład)

- Włamywanie się do systemów („Hakowanie” systemów)

Moduł 6 SYSTEM HACKING - zajęcia praktyczne (ćwiczenia)

- Zagrożenia malware – rodzaje niebezpiecznego oprogramowania i mechanizmy działania

Moduł 7 Podsłuchiwanie sieci – przechwytywanie danych - zajęcia praktyczne (ćwiczenia)

Moduł 8 Socjotechniki (Inżynieria społeczna) - zajęcia teoretyczne (wykład)

Moduł 9 Ataki na odmowę dostępu do usługi - zajęcia teoretyczne (wykład)

Moduł 10 Przechwytywanie sesji – przejęcie komunikacji między ofiarą a systemem docelowym - zajęcia praktyczne (ćwiczenia)

Moduł 11 Omijanie systemów IDS, firewall'i, honeypot'ów - zajęcia praktyczne (ćwiczenia)

- Atakowanie serwerów webowych

Moduł 12 Atakowanie aplikacji webowych - zajęcia teoretyczne (wykład)

- SQL Injection – ataki z wykorzystaniem braku odpowiedniego filtrowania zapytań baz danych SQL

Moduł 13 Włamywanie się do sieci bezprzewodowych - zajęcia praktyczne (ćwiczenia)

Moduł 14 Hakowanie platform i urządzeń mobilnych - zajęcia praktyczne (ćwiczenia)

- Hakowanie "Internetu Rzeczy" (IoT)

Moduł 15 Koncepcje i bezpieczeństwo rozwiązań chmurowych (cloud computing) - zajęcia praktyczne (ćwiczenia)

- CRYPTOGRAPHY - Kryptografia
- Walidacja

Szkolenie trwa 40 godzin lekcyjnych

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	8 474,70 PLN
Koszt przypadający na 1 uczestnika netto	6 890,00 PLN
Koszt osobogodziny brutto	211,87 PLN
Koszt osobogodziny netto	172,25 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Dawid Koziorowski

Doświadczenie zawodowe: trener w Dagma Szkolenia IT z zakresu cyberbezpieczeństwa, prowadzący wdrożenia i kursy z tematyki CEH - Certified Ethical Hacker v12. Posiada minimum trzyletnie doświadczenie w dziedzinie szkolenia.
Certyfikowany trener CEH; wykształcenie wyższe

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

- materiały dydaktyczne w formie elektronicznej (materiały dydaktyczne dostępne na platformie EC COUNCIL, do których dostęp jest przesyłany na e-mail uczestnika)
- dostęp do przygotowanego środowiska wirtualnego (dane dostępowe przesłane na wskazany przez uczestnika adres e-mail)

Warunki uczestnictwa

Prosimy o zapisanie się na szkolenie przez naszą stronę internetową **https://szkolenia.dagma.eu/pl** w celu rezerwacji miejsca.

Wymagania sprzętowe:

- komputer z aktualnym systemem operacyjnym Microsoft Windows lub macOS.
- aktualna wersja przeglądarki internetowej zgodnej z HTML5,

Opcjonalnie:

- minimalna rozdzielczość ekranu 1920 x 1080,
- tablet lub inne urządzenie, na którym będziesz mógł przeglądać materiały.

Informacje dodatkowe

- **Jedna godzina szkolenia to 45 minut**
- W cenę szkolenia nie wchodzą koszta związane z dojazdem, wyżywieniem oraz noclegiem.
- Uczestnik otrzyma zaświadczenie DAGMA Szkolenia IT o ukończeniu szkolenia
- Uczestnik ma możliwość złożenia reklamacji po zrealizowanej usłudze, sporządzając ją w formie pisemnej (na wniosku reklamacyjnym) i odsyłając na adres szkolenia@dagma.pl. Reklamacja zostaje rozpatrzona do 30 dni od dnia otrzymania dokumentu przez DAGMA Szkolenia IT

Warunki techniczne

WARUNKITECHNICZNE:

a) platforma/rodzaj komunikatora, za pośrednictwem którego prowadzona będzie usługa:

- **ZOOM**
- w przypadku kilku uczestników przebywających w jednym pomieszczeniu, istnieją dwie możliwości udziału w szkoleniu:

1) każda osoba bierze udział w szkoleniu osobno (korzystając z oddzielnych komputerów), wówczas należy wyciszyć dźwięki z otoczenia by uniknąć sprzężeń;

2) otrzymujecie jedno zaproszenie, wówczas kilka osób uczestniczy w szkoleniu za pośrednictwem jednego komputera

- Można łatwo udostępniać sobie ekran, oglądać pliki, bazę handlową, XLS itd.

b) minimalne wymagania sprzętowe, jakie musi spełniać komputer Uczestnika lub inne urządzenie do zdalnej komunikacji:

- Uczestnik potrzebuje komputer z przeglądarką Chrome lub Edge (NIE firefox), mikrofon, głośniki.

c) minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować Uczestnik:

- łącze internetowe o przepustowości minimum 10Mbit,

d) niezbędne oprogramowanie umożliwiające Uczestnikom dostęp do prezentowanych treści i materiałów:

- uczestnik na tydzień przed szkoleniem otrzyma maila organizacyjnego, ze szczegółową instrukcją pobrania darmowej platformy ZOOM.
- Z platformy MS Teams można korzystać za pośrednictwem przeglądarki, nie trzeba nic instalować.

e) okres ważności linku:

- link będzie aktywny od pierwszego dnia rozpoczęcia się szkolenia do ostatniego dnia trwania usługi

Szczegóły, związane z prowadzonymi przez nas szkoleniami online, znajdziesz na naszej stronie: https://szkolenia.dagma.eu/pl/training-list

Kontakt

Agnieszka Palenga

E-mail palenga.a@dagma.pl

Telefon (+48) 32 7931 139