Możliwość dofinansowania

Dagma sp. z o.o.

★★★★½

Techniki hackingu i cyberprzestępczości - Poziom 3 Ataki na strony i aplikacje webowe

Numer usługi 2024/07/03/17164/2207126

zdalna w czasie rzeczywistym
Usługa szkoleniowa
21 h
21.08.2024 do 23.08.2024

5 768,70 PLN brutto
4 690,00 PLN netto
274,70 PLN brutto/h
223,33 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Szkolenie przeznaczone jest dla osób pracujących w sektorze IT, spełniających poniższe wymagania: • Znajomosc podstaw Linuxa, działania sieci, zasady działania systemów • Wiedza ze szkolenia **Techniki hackingu i cyberprzestępczości - Poziom 2 Ataki na systemy i sieci**
Minimalna liczba uczestników	4
Maksymalna liczba uczestników	8
Data zakończenia rekrutacji	14-08-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	21
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 „Technik hackingu i cyberprzestępczości - Poziom 3 Ataki na strony i aplikacje webowe" przygotowuje do skutecznego rozpoznawania ataków na aplikacje webowe i strony www oraz przeciwdziałaniu metodom atakowania i włamywania się do systemów informatycznych przez luki w oprogramowaniu www, w związku z czym uczestnik jest w stanie w pełni zabezpieczyć systemy operacyjne oraz sieci informatyczne swojej firmy.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik zabezpiecza systemy operacyjne oraz sieci informatyczne; stosuje i broni się przed nowoczesnymi technikami internetowych włamywaczy;	samodzielna praca i wykonywanie zadań w środowisku wirtualnym podczas szkolenia	Obserwacja w warunkach rzeczywistych
Uczestnik dobiera właściwe metody ochrony przed cyberatakami samodzielnie rozpoznaje ataki na aplikacje webowe i strony www	samodzielna praca i wykonywanie zadań w środowisku wirtualnym podczas szkolenia	Obserwacja w warunkach rzeczywistych
Uczestnik nabędzie kompetencje społeczne, takie jak samokształcenie, rozwiązywanie problemów, kreatywność w działaniu.	samodzielna praca i wykonywanie zadań w środowisku wirtualnym podczas szkolenia	Obserwacja w warunkach rzeczywistych

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 tematyki ataków na strony internetowe i aplikacje webowe - zajęcia teoretyczne (wykład)

- Głębokie ukrycie

Moduł 2 Insecure Logins Forms - zajęcia teoretyczne (wykład)

- Logout Management

Moduł 3 Password Attack - zajęcia praktyczne (ćwiczenia)

- Account Lockout

Moduł 4 Web Parameter Tampering - zajęcia praktyczne (ćwiczenia)

- Path oraz Information Disclosure

Moduł 5 Path Traversal - zajęcia teoretyczne (wykład)

- Local File Inclusion

Moduł 6 Remote File Inclusion - zajęcia praktyczne (ćwiczenia)

- Omijanie filtrowania danych

Moduł 7 Command Injection (+ Blind) - zajęcia teoretyczne (wykład)

- Sessions Management

Moduł 8 Upload File - zajęcia praktyczne (ćwiczenia)

- CSRF - Cross Site Request Forgery

Moduł 9 SQL Injection - GET, POST - zajęcia praktyczne (ćwiczenia)

- XSS Attack - Reflected, Stored
- Automatyzacja SQL Injection

Godzinowy harmonogram usługi ma charakter orientacyjny - trener, w zależności od potrzeb uczestników, może zmienić długość poszczególnych modułów (przy zachowaniu łącznego wymiaru 21 godz. lekcyjnych). Podczas szkolenia, w zależności od potrzeb uczestników, będą robione krótkie przerwy. Trener ustali z uczestnikami konkretne godziny przerw.

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	5 768,70 PLN
Koszt przypadający na 1 uczestnika netto	4 690,00 PLN

Koszt osobogodziny brutto	274,70 PLN
Koszt osobogodziny netto	223,33 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Daniel Suchocki

Doświadczenie zawodowe: Posiada 15-letnie doświadczenie w bezpieczeństwie systemów i sieci informatycznych oraz 9 letnie doświadczenie w informatyce śledczej. Trener IT w autoryzowanym centrum szkoleniowym Dagma od 2017 roku.
Wieloletnie doświadczenie w prowadzeniu szkoleń, wykładów i konsultacji w dziedzinie technik hackingu, informatyki śledczej, technik cyberprzestępczości, przeciwdziałaniu atakom na strony, aplikacje webowe, systemy i rozwiązania chmurowe. Zna teoretyczne aspekty zagadnień i posiada minimum trzyletnie doświadczenie dydaktyczne oraz praktyczne w dziedzinie. Certyfikowany trener CEH.
Wykształcenie wyższe.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

- materiały dydaktyczne w formie elektronicznej (e-book, lub dostęp do materiałów autorskich, przygotowanych przez trenera, przesłany na adres mailowy uczestnika)
- dostęp do przygotowanego środowiska wirtualnego

Warunki uczestnictwa

Prosimy o zapisanie się na szkolenie przez naszą stronę **www.acsdagma.com.pl** w celu rezerwacji miejsca.

Informacje dodatkowe

Informacje organizacyjne:

- Jedna godzina lekcyjna to 45 minut
- W cenę szkolenia nie wchodzą koszta związane z dojazdem, wyżywieniem oraz noclegiem.
- Szkolenie nie zawiera egzaminu.
- Uczestnik otrzyma zaświadczenie ACS 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 Autoryzowane Centrum Szkoleniowe DAGMA.

Warunki techniczne

WARUNKITECHNICZNE:

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

- **ZOOM i/lub MS Teams**
- 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 (czyt. od 26 czerwca do 28 czerwca)

Szczegóły, związane z prowadzonymi przez nas szkoleniami online, znajdziesz na naszej stronie:
https://www.acsdagma.com/pl/szkolenia-online

Kontakt

Agnieszka Palenga

E-mail palenga.a@dagma.pl
Telefon (+48) 32 7931 139