Możliwość dofinansowania

Dagma sp. z o.o.

★★★★½

TECHNIKI HACKINGU I CYBERPRZESTĘPCZOŚCI - POZIOM 2 ATAKI NA SYSTEMY I SIECI

Numer usługi 2024/07/03/17164/2207125

zdalna w czasie rzeczywistym
Usługa szkoleniowa
21 h
21.08.2024 do 23.08.2024

5 645,70 PLN brutto
4 590,00 PLN netto
268,84 PLN brutto/h
218,57 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 1 Wprowadzenie do hackingu w praktyce**
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 „TECHNIKI HACKINGU I CYBERPRZESTĘPCZOŚCI - POZIOM 2 ATAKI NA SYSTEMY I SIECI” przygotowuje do samodzielnego dobierania właściwych metod ochrony przed konkretnymi cyberatakami, poprzez analizę przebiegu cyberataku i neutralizowaniu go w zarodku. Uczestnik skutecznie zabezpiecza firmowe infrastruktury IT oraz urządzenia w sieci teleinformatycznej przed atakami na systemy operacyjne.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik skutecznie zabezpiecza urządzenia w sieci teleinformatycznej; analizuje przebieg cyberataków; zna nowoczesne techniki internetowych włamywaczy;	samodzielna praca i wykonywanie zadań w środowisku wirtualnym podczas szkolenia	Obserwacja w warunkach rzeczywistych
Uczestnik skutecznie zabezpiecza firmowe infrastruktury IT przed atakami na systemy operacyjne; rozumie sposób działania cyberprzestępców; skutecznie broni się przed atakami; stosuje najlepsze metody przeciwdziałania i zapobiegania atakom.	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 WHOIS i wyliczanie DNS - zajęcia teoretyczne (wykład)

1. Wykorzystywanie zaawansowanego oprogramowania do automatyzacji pracy

Moduł 2 Wehikuł czasu stron internetowych - zajęcia praktyczne (ćwiczenia)

1. Budowa własnych pakietów od podstaw
2. Zaawansowane skanowanie jednostek w warstwie 2, 3 i 4 z wykorzystaniem szerokiej gamy dostępnych narzędzi

Moduł 3 Identyfikowanie usług sieciowych oraz banerów aplikacji - zajęcia teoretyczne (wykład)

1. Identyfikacja systemów oraz zapór sieciowych

Moduł 4 Skanowanie TCP / UDP / zombie - zajęcia teoretyczne (wykład)

1. Ataki na systemy operacyjne Windows, Linux, MacOS
2. Atakowanie poprzez błędy w oprogramowaniu JAVA, Winamp, Flash DLL

Moduł 5 Szybka identyfikacja możliwych ataków - Windows Exploit Suggester - zajęcia praktyczne (ćwiczenia)

1. Ataki na powłokę bash – BashShelshock

Moduł 6 Hakowanie kiosków internetowych - zajęcia praktyczne (ćwiczenia)

1. Ataki DoS/DDoS z wykorzystaniem serwerów DNS (DNS amplification)

Moduł 7 Ataki DoS/DDoS typu buffer overflow - zajęcia praktyczne (ćwiczenia)

1. Ataki DoS/DDoS syn Flood
2. Ataki DoS/DDoS Sockstress

Moduł 8 Omijanie blokad w sieci metodą tunelowania połączeń - zajęcia teoretyczne (wykład)

1. Ataki Honeypot i Misassociation
2. Ataki Hirte

Moduł 9 Ataki na protokół PEAP - zajęcia praktyczne (ćwiczenia)

1. Ataki na protokół EAP-TTLS
2. Ataki socjotechniczne

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	5 645,70 PLN
Koszt przypadający na 1 uczestnika netto	4 590,00 PLN
Koszt osobogodziny brutto	268,84 PLN
Koszt osobogodziny netto	218,57 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) przesyłany na adres mailowy uczestnika
- dostęp do przygotowanego środowiska wirtualnego

Warunki uczestnictwa

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

Laptop/ komputer, na którym będziesz pracował, powinien mieć zainstalowany Virtual Box wraz z dodatkami (extension pack) oraz posiadać około 50 GB wolnej przestrzeni dyskowej i minimum 4 GB RAM.

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 27 grudnia do 29 grudnia)

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