



Dagma sp. z o.o.

★★★★★ 4,5 / 5

420 ocen

CEH - Certified Ethical Hacker v13 AI

Numer usługi 2025/02/28/17164/2588597

📍 zdalna w czasie rzeczywistym

🏠 Usługa szkoleniowa

🕒 40 h

📅 22.09.2025 do 26.09.2025

8 966,70 PLN brutto

7 290,00 PLN netto

224,17 PLN brutto/h

182,25 PLN netto/h

Informacje podstawowe

Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

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

12

Data zakończenia rekrutacji

15-09-2025

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, 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
Efekty dotyczące wiedzy: Uczestnik stosuje obowiązujące normy i standardy bezpieczeństwa.	Tworzy polityki na urządzeniach IDS/IPS dotyczących wykrywania włamań.	Obserwacja w warunkach symulowanych
Efekty dotyczące umiejętności: Uczestnik zapobiega metodom eskalacji uprawnień w systemach firmowych.	Skanuje, testuje i przełamuje zabezpieczenia systemów	Obserwacja w warunkach symulowanych
Efekty dotyczące kompetencji społecznych: uczestnik buduje relacje społeczne.	Projektuje działania w oparciu o zasady empatii, budowania zaufania i efektywnej komunikacji	Wywiad swobodny

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 Podśluchiwanie 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

Razem 40 godzin lekcyjnych, (30 godzin zegarowych):

- walidacja jest wliczona w czas szkolenia / przerwy

nie są

wliczone w czas trwania szkolenia.

Harmonogram

Liczba przedmiotów/zajęć: 16

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 16 Moduł 1 Wprowadzenie do „Etycznego Hackingu” - zajęcia teoretyczne (wykład)	Daniel Rozwadowski	22-09-2025	09:00	10:30	01:30
2 z 16 Moduł 2 Wstępne zbieranie informacji o celu ataku - zajęcia teoretyczne (wykład)	Daniel Rozwadowski	22-09-2025	10:45	13:00	02:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
3 z 16 Moduł 3 Skanowanie sieci - identyfikacja systemów, portów, usług działających w sieci - zajęcia praktyczne (ćwiczenia)	Daniel Rozwadowski	22-09-2025	13:30	15:45	02:15
4 z 16 Moduł 4 Enumeracja - zajęcia teoretyczne (wykład)	Daniel Rozwadowski	23-09-2025	09:00	10:30	01:30
5 z 16 Moduł 5 Analiza podatności - omówienie narzędzi do wykonywania skanowania oraz kryteriów ich doboru - zajęcia teoretyczne (wykład)	Daniel Rozwadowski	23-09-2025	10:45	13:00	02:15
6 z 16 Moduł 6 SYSTEM HACKING - zajęcia praktyczne (ćwiczenia)	Daniel Rozwadowski	23-09-2025	13:30	15:45	02:15
7 z 16 Moduł 7 Podśluchiwanie sieci – przechwytywanie danych - zajęcia praktyczne (ćwiczenia)	Daniel Rozwadowski	24-09-2025	09:00	10:30	01:30
8 z 16 Moduł 8 Socjotechniki (Inżynieria społeczna) - zajęcia teoretyczne (wykład)	Daniel Rozwadowski	24-09-2025	10:45	13:00	02:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
9 z 16 Moduł 9 Ataki na odmowę dostępu do usługi - zajęcia teoretyczne (wykład)	Daniel Rozwadowski	24-09-2025	13:30	15:45	02:15
10 z 16 Moduł 10 Przechwytywanie sesji – przejęcie komunikacji między ofiarą a systemem docelowym - zajęcia praktyczne (ćwiczenia)	Michał Janik	25-09-2025	09:00	10:30	01:30
11 z 16 Moduł 11 Omijanie systemów IDS, firewall'i, honeypot'ów - zajęcia praktyczne (ćwiczenia)	Michał Janik	25-09-2025	10:45	13:00	02:15
12 z 16 Moduł 12 Atakowanie aplikacji webowych - zajęcia teoretyczne (wykład)	Michał Janik	25-09-2025	13:30	15:45	02:15
13 z 16 Moduł 13 Włamywanie się do sieci bezprzewodowych - zajęcia praktyczne (ćwiczenia)	Michał Janik	26-09-2025	09:00	10:30	01:30
14 z 16 Moduł 14 Hakowanie platform i urządzeń mobilnych - zajęcia praktyczne (ćwiczenia)	Michał Janik	26-09-2025	10:45	13:00	02:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
15 z 16 Moduł 15 Konceptcje i bezpieczeństwo rozwiązań chmurowych (cloud computing) - zajęcia praktyczne (ćwiczenia)	Michał Janik	26-09-2025	13:30	15:25	01:55
16 z 16 WALIDACJA	-	26-09-2025	15:25	15:45	00:20

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	8 966,70 PLN
Koszt przypadający na 1 uczestnika netto	7 290,00 PLN
Koszt osobogodziny brutto	224,17 PLN
Koszt osobogodziny netto	182,25 PLN

Prowadzący

Liczba prowadzących: 2



1 z 2

Daniel Rozwadowski

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



2 z 2

Michał Janik

Obszar specjalizacji: Aplikacje typu Antywirus, szyfrowanie, DLP, MDM, Antyspam dla serwera pocztowego, CEH Doświadczenie zawodowe: specjalista, a następnie inżynier systemowy w firmie

Dagma. Doświadczenie w świadczeniu tego typu usług: Zna teoretyczne aspekty zagadnień i posiada minimum trzyletnie doświadczenie dydaktyczne oraz praktyczne w dziedzinie.
Wykształcenie: wyższe, magister inżynier Informatyki.

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 wchodzi koszt związany 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 Sp. z o.o.
- Podstawa zwolnienia z VAT: dofinansowanie w co najmniej 70% - zgodnie z treścią § 3 ust. 1 pkt 14 Rozporządzenia Ministra Finansów z dnia 20.12.2013r. 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

WARUNKI TECHNICZNE:

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