Możliwość dofinansowania

Techniki hackingu i cyberprzestępczości - Etyczny Hacking w praktyce - poziom 1

Numer usługi 2026/05/28/17164/3593336

5 768,70 PLN brutto
4 690,00 PLN netto
274,70 PLN brutto/h
223,33 PLN netto/h
261,33 PLN cena rynkowa

Dagma sp. z o.o.

4,5 / 5

456 ocen

Usługa szkoleniowa
zdalna w czasie rzeczywistym
Zajęcia grupowe
21:00 h
20.07.2026 do 22.07.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie przeznaczone jest dla osób pracujących w sektorze IT, spełniających poniższe wymagania: • znajomość podstaw Linuxa, • znajomość podstaw administracji sieci komputerowych, • znajomość modelu ISO/OSI, • znajomość podstaw protokołów IP, TCP, UDP, DHCP, DNS, ARP, • znajomość podstaw sieci bezprzewodowych oraz ich metod zabezpieczania.
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	13-07-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
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 techniki hackingu i cyberprzestępczości, dzięki którym uczestnik będzie samodzielnie rozpoznawał i zapobiegał technikom jakimi posługują się przestępcy w cyfrowym świecie; bronił przed atakami na systemy operacyjne, znał postincydentalne sposoby analizy skompromitowanych

jednostek w sieci. Uczestnik po ukończonym szkoleniu nabędzie kompetencje społeczne takie jak samokształcenie, rozwiązywanie problemów.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
skutecznie zabezpiecza urządzenia w sieci teleinformatycznej,	uczestnik analizuje przebieg cyberataków i zna nowoczesne techniki internetowych włamywaczy	Obserwacja w warunkach symulowanych
Skuteczne zabezpiecza firmową infrastrukturę IT przed atakami na systemy operacyjne rozumie sposoby działania cyberprzestępców	skutecznie obrania przed atakami stosuje najlepsze metody przeciwdziałania i zapobiegania atakom	Obserwacja w warunkach symulowanych
Uczestnik nabędzie kompetencje społeczne, takie jak samokształcenie, rozwiązywanie problemów, kreatywność w działaniu.	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 lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Moduł 1 Fingerprinting - informacje uzyskiwane z sieci Internet - zajęcia teoretyczne (wykład)

1. Google Hacking
2. Podstawowe skanowanie urządzeń w sieci

Moduł 2 Zaawansowane skanowanie urządzeń w sieci - zajęcia praktyczne (ćwiczenia)

1. Identyfikowanie usług sieciowych oraz banerów aplikacji
2. Identyfikacja systemów oraz zapór sieciowych

Moduł 3 Ataki na system operacyjny Windows - zajęcia teoretyczne (wykład)

1. Ataki na bazy danych

Moduł 4 Ataki na przeglądarki internetowe - zajęcia praktyczne (ćwiczenia)

1. Atakowanie poprzez błędy w oprogramowaniu
2. Ataki na system operacyjny Linux

Moduł 5 Ataki socjotechniczne - zajęcia teoretyczne (wykład)

1. Fałszowanie śladów w zaatakowanym systemie
2. Atak z użyciem techniki pivotingu i port forwarding

Moduł 6 Audytowanie systemów operacyjnych pod kątem podatności - zajęcia praktyczne (ćwiczenia)

1. Port knocking

Moduł 7 Ataki na sieci bezprzewodowe - zajęcia teoretyczne (wykład)

1. Ataki na WPS
2. Ataki na WEP

Moduł 8 Ataki na WPA/WPA2 - zajęcia praktyczne (ćwiczenia)

1. Ataki z użyciem tęczowych tablic
2. Ataki z użyciem akceleracji graficznej

Moduł 9 Generatory słowników - zajęcia praktyczne (ćwiczenia)

1. Crackowanie hashy
2. Automatyzacja ataków na sieci bezprzewodowe

Walidacja

· Walidacja jest wliczona w czas trwania szkolenia.

· Przerwy nie są wliczone w czas trwania szkolenia

Harmonogram

Liczba pozycji harmonogramu: 21

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 21 Moduł 1 Fingerprinting - informacje uzyskiwane z sieci Internet - zajęcia teoretyczne (wykład)	Zajęcia	Armand Pajor	20-07-2026	09:00	11:00	02:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
2 z 21 -	Przerwa	-	20-07-2026	11:00	11:15	00:15
3 z 21 Moduł 2 Zaawansowane skanowanie urządzeń w sieci - zajęcia praktyczne (ćwiczenia)	Zajęcia	Armand Pajor	20-07-2026	11:15	13:30	02:15
4 z 21 -	Przerwa	-	20-07-2026	13:30	14:00	00:30
5 z 21 Moduł 3 Ataki na system operacyjny Windows - zajęcia teoretyczne (wykład)	Zajęcia	Armand Pajor	20-07-2026	14:00	15:00	01:00
6 z 21 -	Przerwa	-	20-07-2026	15:00	15:15	00:15
7 z 21 Moduł 3 Ataki na system operacyjny Windows - zajęcia teoretyczne (wykład cz.2)	Zajęcia	Armand Pajor	20-07-2026	15:15	16:00	00:45
8 z 21 Moduł 4 Ataki na przeglądarki internetowe - zajęcia praktyczne (ćwiczenia)	Zajęcia	Armand Pajor	21-07-2026	09:00	10:45	01:45
9 z 21 -	Przerwa	-	21-07-2026	10:45	11:00	00:15
10 z 21 Moduł 5 Ataki socjotechniczne - zajęcia teoretyczne (wykład)	Zajęcia	Armand Pajor	21-07-2026	11:00	13:00	02:00
11 z 21 -	Przerwa	-	21-07-2026	13:00	13:30	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
12 z 21 Moduł 6 Audytowanie systemów operacyjnych pod kątem podatności - zajęcia praktyczne (ćwiczenia)	Zajęcia	Armand Pajor	21-07-2026	13:30	14:45	01:15
13 z 21 -	Przerwa	-	21-07-2026	14:45	15:00	00:15
14 z 21 Moduł 6 Audytowanie systemów operacyjnych pod kątem podatności - zajęcia praktyczne (ćwiczenia cz.2)	Zajęcia	Armand Pajor	21-07-2026	15:00	16:00	01:00
15 z 21 Moduł 7 Ataki na sieci bezprzewodowe - zajęcia teoretyczne (wykład)	Zajęcia	Armand Pajor	22-07-2026	09:00	11:15	02:15
16 z 21 -	Przerwa	-	22-07-2026	11:15	11:30	00:15
17 z 21 Moduł 8 Ataki na WPA/WPA2 - zajęcia praktyczne (ćwiczenia)	Zajęcia	Armand Pajor	22-07-2026	11:30	13:30	02:00
18 z 21 -	Przerwa	-	22-07-2026	13:30	14:00	00:30
19 z 21 Moduł 9 Generatory słowników - zajęcia praktyczne (ćwiczenia)	Zajęcia	Armand Pajor	22-07-2026	14:00	15:15	01:15
20 z 21 -	Przerwa	-	22-07-2026	15:15	15:30	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
21 z 21 -	Walidacja	-	22-07-2026	15:30	16:00	00:30

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	21:00
w tym suma godzin zajęć	17:30
w tym suma godzin walidacji	00:30
w tym suma przerw	03:00
Suma godzin dydaktycznych bez przerw	24:00

Cennik

Jeżeli korzystasz z dofinansowania i usługa stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego wraz z usługą lub dostawą towarów ściśle związaną z usługami kształcenia zawodowego lub przekwalifikowania zawodowego to możesz mieć możliwość skorzystania za zwolnienia z podatku VAT na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2024 r. o podatku od towarów i usług, jeśli usługa w całości jest finansowana ze środków publicznych lub § 3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień w przypadku, gdy usługa jest finansowana w co najmniej 70% ze środków publicznych.

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

Liczba godzin usługi

Rodzaj godzin	Liczba godzin

Liczba godzin zegarowych usługi	21:00

Prowadzący

Liczba prowadzących: 1

1 z 1

Armand Pajor

Doświadczenie zawodowe: Trener IT, prowadzący szkolenia w Dagma Szkolenia IT od początku 2023 roku. Wdrożeniowiec i analityk cyberbezpieczeństwa sieci. Prowadzący autorskie szkolenie firmy FORSEC z zakresu Technik hackingu oraz Cyberbezpieczeństwa sieci (Lan Security Analyst) i systemów operacyjnych (OS Security Analyst)
Uzyskane certyfikacje: ITIL Foundation Certificate in IT Service Management, Corporate Readiness Certificate - Information Security Management, Corporate Readiness Certificate - Troubleshooting
Specjalizacja: Sieci komputerowe, Cyberbezpieczeństwo, Network Traffic Analysis, Cyber Threat Hunting (CTH), C#, Python, Java
Wykształcenie: wyższe, Politechnika Krakowska, magister Informatyki

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

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

Warunki uczestnictwa

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

Informacje dodatkowe

Informacje organizacyjne:

· Harmonogram ma charakter orientacyjny. Trener może zmienić długość trwania poszczególnych modułów zgodnie z zapotrzebowaniem grupy (przy zachowaniu niezmienionego wymiaru czasu dnia szkoleniowego tj. 7 godzin zegarowych włączając przerwy).

· W cenę szkolenia nie wchodzą koszty 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 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

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 20 grudnia do 22 grudnia)

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

Kontakt

Michalina Krzyszkowska

E-mail krzyszkowska.m@dagma.pl
Telefon (+48) 327 931 015