Możliwość dofinansowania

CEH - Certified Ethical Hacker v13

Numer usługi 2026/02/02/10100/3301884

8 000,00 PLN brutto
8 000,00 PLN netto
200,00 PLN brutto/h
200,00 PLN netto/h

Compendium - Centrum Edukacyjne Spółka z o.o.

4,3 / 5
190 ocen

Usługa szkoleniowa
zdalna w czasie rzeczywistym
40:00 h
22.06.2026 do 26.06.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT

Grupa docelowa usługi	**Komu w szczególności polecamy CEH v13**:
	• **Specjalistom ds. cyberbezpieczeństwa**
	  • Wszystkim tym, którzy chcą rozwijać swoją karierę w cyberbezpieczeństwie
	• **Zespołom IT i organizacjom, które stawiają na bezpieczeństwo swoich systemów IT**
	  • Całym zespołom IT, które chcą zwiększyć swoją wiedzę na temat cyberbezpieczeństwa, a w szczególności technik stosowanych przez atakujących i czy sposobów testowania bezpieczeństwa i ochrony w wykorzystaniem AI, tak aby być o krok przed złośliwymi aktorami.
	• **Kadrze pracującej w instytucjach rządowych i wojskowych**
	Osoby pracujące w instytucjach rządowych i organach obronnych w szczególności powinny poświadczać swoje umiejętności w oparciu o globalnie rozpoznawalne i zaufane programy edukacyjne i certyfikacyjne.

Minimalna liczba uczestników	4
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	21-06-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	40

Podstawa uzyskania wpisu do BUR	Znak Jakości Małopolskich Standardów Usług Edukacyjno-Szkoleniowych (MSUES) - wersja 2.0

Cel

Cel edukacyjny

Szkolenie dostarcza kompetencji uczestnikowi do samodzielnego dokonywania kontrolowanych włamań do systemu „ofiary", identyfikowania słabych punktów w organizacji, skanowania oraz testowania i przełamywania zabezpieczenia systemów.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozumie jak korzystać oraz co znaczy Etyczne hakowanie.	Aktywnie i ze zrozumieniem: korzysta z kwestii związanych z bezpieczeństwem informacji, w tym podstaw etycznego hakowania, kontroli bezpieczeństwa informacji, właściwych przepisów i standardowych procedur.	Wywiad swobodny
Rozumie jak działa i jak korzystać z Foot Printing i rekonesansu.	Przegląda i korzysta z najnowszych technik i narzędzi do przeprowadzania foot printingu i rekonesansu, kluczowej fazy poprzedzającej atak w procesie etycznego hakowania.	Wywiad swobodny
Rozpoznaje i korzysta z Enumeracji, Analizy podatności, Hakowania systemów.	Kontroluje i zarządza technikami enumeracji, między innym takich jak eksploatacja Border Gateway Protocol (BGP) i Network File Sharing (NFS), oraz odpowiednich środków zaradczych. Identyfikuje luki w zabezpieczeniach sieci, infrastruktury komunikacyjnej i systemów końcowych docelowej organizacji. Przedstawienie różnych rodzajów oceny podatności i narzędzi do ich oceny.	Wywiad swobodny
Rozpoznaje i korzysta z technik Hakowania systemów	Korzysta z technik hakowania systemów, w tym steganografii, ataków steganograficznych i ukrywania śladów, używanych do odkrywania luk w systemach i sieciach.	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 hakowania**
- **Moduł 2 - Foot Printing i rekonesans**
- **Moduł 3 - Skanowanie sieci**
- **Moduł 4 - Enumeracja**
- **Moduł 5 - Analiza podatności**
- **Moduł 6 - Hakowanie systemów**
- **Moduł 7 - Zagrożenia typu malware**
- **Moduł 8 - Sniffing**
- **Moduł 9 - Socjotechnika**
- **Moduł 10 - Ataki typu Denial-of-Service**
- **Moduł 11 - Przejęcie sesji**
- **Moduł 12 - Omijanie IDS, zapór sieciowych czy sytemów typu honeypot**
- **Moduł 13 - Hakowanie serwerów www**
- **Moduł 14 - Hakowanie aplikacji www**
- **Moduł 15 - Wstrzykiwanie SQL**
- **Moduł 16 - Hakowanie sieci bezprzewodowych**
- **Moduł 17 - Hakowanie platform mobilnych**
- **Moduł 18 - Hakowanie IoT i OT**
- **Moduł 19 - Przetwarzanie w chmurze**

Moduł 20 - Kryptografia

Harmonogram

Liczba pozycji harmonogramu: 0

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	8 000,00 PLN
Koszt przypadający na 1 uczestnika netto	8 000,00 PLN
Koszt osobogodziny brutto	200,00 PLN
Koszt osobogodziny netto	200,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Miłosz Jaworski

Pasjonat wszystkiego, co kryje się pod pojęciem IT Security. Inżynier z wieloletnim doświadczeniem ponad 10 lat w zakresie
projektowania infrastruktury sieci przewodowych i bezprzewodowych oraz infrastruktury bezpieczeństwa IT. W
codziennej pracy zajmuje się architekturą sieci i bezpieczeństwa - projektuje, buduje rozwiązania pod dane potrzeby i
wymogi klienta. Dzięki biegłości w znajomości rozwiązań sieciowych oraz bezpieczeństwa systemów IT często
pracujący przy wdrożeniach w roli konsultanta. Jako trener szkoli z technologii zaawansowanych, jest również
autorem wielu publikacji i filmów instruktażowych dotyczących nowinek technologicznych. Autoryzowany Trener.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Autoryzowane materiały szkoleniowe.

Warunki techniczne

Szkolenie obywa się za pośrednictwem platformy **Microsoft Teams.**

Uczestnik może zadawać pytania i aktywnie uczestniczyć w dyskusji. Uczestnik, który potwierdzi swój udział w szkoleniu, przed rozpoczęciem szkolenia, drogą mailową, otrzyma link do spotkania wraz z hasłami dostępu.

Wymagania sprzętowe:

- komputer z dostępem do internetu o minimalnej przepustowości 10Mb/s.

- urządzenie do obsługi audio - słuchawki/glosniki oraz mikrofon.

- zainstalowana dowolna przeglądarka internetowa - np. **Google Chrome**

Kontakt

MICHAŁ DOBRZAŃSKI

E-mail michal.dobrzanski@compendium.pl
Telefon (+48) 122 984 777