Szkolenie: EC-Council
CEH - Certified Ethical Hacker v13

EC-Council Building A Culture Of Security

DOSTĘPNE TERMINY

2024-11-18 | 5 dni | Virtual Classroom
2024-12-02 | 5 dni | Warszawa / Wirtualna sala *(Promocja, Termin gwarantowany, Rabat -2300 PLN)*
2024-12-09 | 5 dni | Virtual Classroom
2024-12-09 | 5 dni | Warszawa / Wirtualna sala
2025-01-27 | 5 dni | Virtual Classroom
2025-01-27 | 5 dni | Warszawa / Wirtualna sala
2025-03-24 | 5 dni | Virtual Classroom
2025-03-24 | 5 dni | Warszawa / Wirtualna sala

Cel szkolenia:

C|EH Certified Ethical Hacker

Certified Ethical Hacker (C|EH®) to globalnie rozpoznawalne i uznane w branży szkolenie i certyfikacja od EC-Council. W swojej 13 wersji szkolenie CEH przynosi nam funkcjonalność AI która z powodzeniem może być wykorzystywana w rutynowych zadaniach wykonywanych prze etyczny hakerów.

- **AI**
  - Pierwszy na świecie program szkoleniowy dotyczący etycznego hakowania, który uczy możliwości wykorzystania AI (sztucznej inteligencji) w zadaniach etycznego hakera
- **Umiejętności praktyczne**
  - Podczas szkolenia jak i również po jego zakończeniu w przypadku wersji Elite można doskonalić swoje umiejętności praktyczne w oparciu o rzeczywiste scenariusze realizowane w środowisku laboratoryjne. Można ćwiczyć różne wektory ataków i opanowywać zaawansowane narzędzia hakerskie.
- **Bądź 40% bardziej wydajny**
  - Poznaj techniki napędzane przez AI, aby zwiększyć wydajność w zakresie obrony

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

cybernetycznej nawet o 40%, jednocześnie usprawniając przepływy pracy.

- **Intensywny, zaktualizowany program nauczania**
  - Opanuj najnowsze zaawansowane techniki ataków, trendy i środki zaradcze.
- **2x większa produktywność**
  - Zaawansowane wykrywanie zagrożeń, ulepszone podejmowanie decyzji, adaptacyjne uczenie się, ulepszone raportowanie i automatyzacja powtarzalnych zadań.
- **Udowodnij swoje umiejętności (wersja Elite)**
  - Uczestnicz w comiesięcznych globalnych konkursach hakerskich, rywalizuj z innymi, zdobywaj punkty i pnij się w górę na tablicy wyników.

Autoryzowany CEH to również wyjątkowy program nauki, składający z czterech elementów: Learn | Certify | Engage | Compete, który skutecznie przygotowuje uczestników do certyfikacji, daje możliwość zdobycia dogłębnej wiedzy i który oferuje dużą ilość praktycznych ćwiczeń, co czyni go jednym z najbardziej wszechstronnym programów edukacyjnych dotyczących cyberbezpieczeństwa dostępnym na rynku.

- **Learn**
  - Rozwijaj umiejętności w kluczowych obszarach cyberbezpieczeństwa dzięki 20 modułom tematycznym. Korzystaj z ponad 220 praktycznych laboratoriów, poznaj 550 technik ataków i ponad 4000 narzędzi przydatnych, każdemu etycznemu hakerowi i specjaliście ds. bezpieczeństwa.
- **Certify**
  - Przystąp do 4-godzinnego egzaminu z 125 pytaniami wielokrotnego wyboru, aby zdobyć tytuł CEH w wersji v13 oraz opcjonalnie do 6-godzinnego egzaminu praktycznego z 20 rzeczywistymi wyzwaniami, aby uzyskać certyfikat CEH Master.

Każdy uczestnik autoryzowanego szkolenia CEH - Certified Ethical Hacker v13 realizowanego w Compendium CE, otrzymuje darmowy voucher egzaminacyjny CEH (MCQ) Certification exam. A w przypadku wersji Elite również voucher na egzamin CEH (Practical).

- **Engage**
  - Zaangażuj się w symulowane etyczne hakowanie. Wyzwanie to wymaga od uczestników krytycznego myślenia oraz testowania wcześniej zdobytej wiedzy i umiejętności w ramach zdobywania „flag”. W ten sposób sprawdzasz realne zastosowanie zdobytych umiejętności i swoje zdolności w odizolowanym środowisku Cyber Range EC-Council co nie prowadzi do żadnych złych konsekwencji.
- **Compete**
  - Rywalizuj z innymi zawodnikami z całego świata, mając roczny dostęp do 12 wyzwań CTF (wersja Elite), z których każde trwa 4 godziny. Pomaga to uczestnikom podnosić swoje

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

umiejętności i być na bieżąco z najnowszymi trendami.

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.

Akredytacje i rekomendacje, które posiada CEH:

- American Council of Education (ACE)
- ANSI National Accreditation Board (ANAB)
- DoD Cyber Workforce Qualification Program
- Army Credentialing Assistance
- National Initiative for Cybersecurity Education (NICE)

Plan szkolenia:

Program szkoleniowy CEH v13 obejmuje 20 modułów, które dotyczą różnych technologii, taktyk i procedur, dostarczając przyszłym etycznym hakerom niezbędnej wiedzy i umiejętności do realizacji ich zadań zawodowych. Każda omawiana taktyka jest wspierana poprzez ćwiczenia laboratoryjne wykonywane w zwirtualizowanym dedykowanym środowisku ćwiczeniowym w którym znajdziemy cele, narzędzia i szereg systemów podatnych na ataki.

- Moduł 1 - Wprowadzenie do etycznego hakowania

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Omówienie podstawowych kwestii związanych z bezpieczeństwem informacji, w tym podstaw etycznego hakowania, kontroli bezpieczeństwa informacji, właściwych przepisów i standardowych procedur.

- Moduł 2 - Foot Printing i rekonesans
  - Nauka korzystania z najnowszych technik i narzędzi do przeprowadzania foot printingu i rekonesansu, kluczowej fazy poprzedzającej atak w procesie etycznego hakowania.
- Moduł 3 - Skanowanie sieci
  - Nauka różnych technik skanowania sieci i środków zaradczych.
- Moduł 4 - Enumeracja
  - Nauka różnych technik enumeracji, między innym takich jak eksploatacja Border Gateway Protocol (BGP) i Network File Sharing (NFS), oraz odpowiednich środków zaradczych.
- Moduł 5 - Analiza podatności
  - Nauka identyfikacji luk w zabezpieczeniach sieci, infrastruktury komunikacyjnej i systemów końcowych docelowej organizacji. Przedstawienie różnych rodzajów oceny podatności i narzędzi do ich oceny.
- Moduł 6 - Hakowanie systemów
  - Nauka różnych możliwych technik hakowania systemów, w tym steganografii, ataków steganograficznych i ukrywania śladów, używanych do odkrywania luk w systemach i sieciach.
- Moduł 7 - Zagrożenia typu malware
  - Różne rodzaje zagrożeń typu malware (trojany, wirusy, robaki itp.), APT i malwar bezplikowy, procedury analizy malware i środków zaradczych przeciwko tego typu zagrożeniom.
- Moduł 8 - Sniffing
  - Nauka technik sniffingu pakietów i ich wykorzystania do odkrywania luk w zabezpieczeniach sieci oraz środków zaradczych przeciwko atakom sniffingowym.
- Moduł 9 - Socjotechnika
  - Nauka koncepcji i technik socjotechnicznych, w tym identyfikacji prób ataków, audytu podatności na poziomie ludzkim czy sugerowanych środków zaradczych przeciwko atakom socjotechnicznym.
- Moduł 10 - Ataki typu Denial-of-Service
  - Nauka różnych technik ataków typu Denial of Service (DoS) i Distributed DoS (DDoS), a także narzędzi używanych do audytu celu i opracowywania środków zaradczych i ochrony przed atakami DoS i DDoS.
- Moduł 11 - Przejęcie sesji
  - Zrozumienie różnych technik przejmowania sesji używanych do odkrywania słabości w zarządzaniu sesjami na poziomie sieci, uwierzytelnianiu, autoryzacji i kryptografii oraz odpowiednich środków zaradczych.
- Moduł 12 - Omijanie IDS, zapór sieciowych czy sytemów typu honeypot
  - Wprowadzenie do technik omijania zapór sieciowych, systemów wykrywania włamań (IDS) i honeypotów; narzędzi używanych do audytu systemów pracujących na brzegu

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

sieci pod kątem identyfikacji ich słabości oraz wypracowania środków zaradczych.

- Moduł 13 - Hakowanie serwerów www
  - Nauka ataków na serwery www, w tym kompleksowej metodyki ataku używanej do audytu luk w infrastrukturze serwerów www oraz odpowiednich środków zaradczych.
- Moduł 14 - Hakowanie aplikacji www
  - Nauka ataków na aplikacje www, w tym kompleksowej metodoyki hakowania aplikacji www używanej do audytu luk w aplikacjach www oraz odpowiednich środków zaradczych.
- Moduł 15 - Wstrzykiwanie SQL
  - Nauka ataków typu SQL injection, technik omijania i środków zaradczych przeciwko SQL injection.
- Moduł 16 - Hakowanie sieci bezprzewodowych
  - Zrozumienie różnych rodzajów technologii bezprzewodowych, w tym szyfrowania, zagrożeń, metodyki hakowania, narzędzi do hakowania, narzędzi do zabezpieczania Wi-Fi i środków zaradczych.
- Moduł 17 - Hakowanie platform mobilnych
  - Nauka wektorów ataku na platformy mobilne, hakowania Androida i iOS, zarządzania urządzeniami mobilnymi, wytycznych dotyczących bezpieczeństwa mobilnego i narzędzi zabezpieczających.
- Moduł 18 - Hakowanie IoT i OT
  - Nauka różnych rodzajów ataków na Internet Rzeczy (IoT) i Technologię Operacyjną (OT), metodyki hakowania, narzędzi do hakowania i środków zaradczych.
- Moduł 19 - Przetwarzanie w chmurze
  - Nauka różnych koncepcji przetwarzania w chmurze, takich jak technologie kontenerowe i przetwarzanie bezserwerowe, różne zagrożenia związane z przetwarzaniem w chmurze, ataki, metodyka hakowania i techniki oraz narzędzia zabezpieczające chmurę.
- Moduł 20 - Kryptografia
  - Nauka algorytmów szyfrowania, narzędzi kryptograficznych, infrastruktury klucza publicznego (PKI), szyfrowania e-maili, szyfrowania dysków, ataków kryptograficznych i narzędzi do kryptanalizy.

Wymagania:

Kurs ten nie wymaga żadnego wcześniejszego doświadczenia w zakresie cyberbezpieczeństwa.

Poziom trudności

Certyfikaty:

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

Uczestnicy szkolenia otrzymują certyfikat ukończenia szkolenia sygnowany przez EC-Council (ukończenie szkolenia). Kurs ten pomoże Ci również przygotować się do egzaminów certyfikacyjnych CEH (MCQ Exam) i CEH (Practical).

CEH (MCQ Multiple Choice Question Exam)

Certified Ethical Hacker (CEH) jest globalnie rozpoznawalnym certyfikatem, uznanym za branżowy standard oceny wiedzy z zakresu etycznego hakowania i testowania bezpieczeństwa. Egzamin certyfikacyjny, akredytowany przez ANAB zgodnie z normą ISO/IEC 17024, składa się z 125 pytań wielokrotnego wyboru, trwa 4 godzinny i jest zdawany pod nadzorem i jest on uznawany na całym świecie jako oryginalny i najbardziej zaufany certyfikat dla etycznych hakerów. Domeny certyfikacyjne są starannie weryfikowane przez praktyków branżowych, co zapewnia, że certyfikat odpowiada aktualnym wymaganiom branżowym; egzamin ten podlega regularnej ocenie psychometrycznej i dostrajaniu, aby zapewnić sprawiedliwą i dokładną ocenę wiedzy kandydata w dziedzinie etycznego hakowania.

CEH (Practical)

Egzamin CEH Practical jest akredytowany przez ANAB zgodnie z normą ISO/IEC 17024. CEH Practical to 6-godzinny, w pełni praktyczny egzamin przeprowadzany w środowisku Cyber Range, który wymaga wykazania się umiejętnościami i zdolnościami praktycznymi w zakresie technik etycznego hakowania, takich jak:

- Narzędzia do skanowania portów (np. Nmap, Hping)
- Wykrywanie podatności
- Ataki na system (np. DoS, DDoS, przechwytywanie sesji, ataki na serwery i aplikacje www, SQL injection, zagrożenia bezprzewodowe)
- Metodyka ataków typu SQL injection i techniki ich unikania
- Narzędzia do zabezpieczania aplikacji www (np. Acunetix WVS)
- Narzędzia do wykrywania podatności typu SQL injection (np. IBM Security AppScan)
- Protokoły komunikacyjne

CEH Practical to drugi krok do uzyskania tytułu CEH Master po zdobyciu certyfikatu CEH. W ramach egzaminu CEH Practical masz ograniczony czas na ukończenie 20 wyzwań, aby przetestować swoje umiejętności i praktyczną biegłość w środowisku Cyber Range. Ten egzamin NIE jest symulacją i obejmuje rzeczywistą sieć korporacyjną z maszynami wirtualnymi i aplikacjami, w której należy wykryć luki w zabezpieczeniach.

CEH Master

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

Po ukończeniu obu części egzaminacyjnych CEH i CEH (Practical), przyznawany jest tytuł CEH (Master). CEH Masters wykazali się biegłością na poziomie mistrzowskim w zakresie wiedzy, umiejętności i zdolności w dziedzinie etycznego hakowania, przechodząc łącznie 10 godzin testów, aby udowodnić swoje kompetencje. Najlepszych 10 uczestników zarówno w egzaminach CEH, jak i CEH Practical jest wyróżnianych na Globalnej Liście Liderów Etycznego Hakowania CEH Master.

Exam Details	CEH (MCQ Exam)	CEH (Practical)
Number of Questions/Practical Challenges	125	20
Test Duration	4 Hours	6 Hours
Test Format	Multiple Choice Questions	iLabs Cyber Range
Test Delivery	ECC EXAM, VUE	-
Availability	-	Aspen-iLabs
Exam Prefix	312-50 (ECC EXAM), 312-50 (VUE)	-
Passing Score	Refer to https://cert.eccouncil.org/faq.html	

Każdy uczestnik autoryzowanego szkolenia CEH - Certified Ethical Hacker v13 realizowanego w Compendium CE, otrzymuje darmowy voucher egzaminacyjny CEH (MCQ) certification exam. A w przypadku wersji Elite również voucher na egzamin CEH (Practical).

Prowadzący:

Certified EC-Council Instructor (CEI)

Informacje dodatkowe:

Chociaż wszystkie dostępne wersje materiałów szkoleniowych do kursu CEHv13 (Lite i Elite) mają pełny dostęp do eCourseware i zawierają voucher na egzamin CEH (MCQ), to jednak wersja Elite oferuje kilka dodatkowych funkcji i materiałów edukacyjnych, które pozwalają pogłębić wiedzę i zdobyć jeszcze więcej praktyczne doświadczenia.

Package Inclusions	C|EH- Elite v13	C|EH v13
eCourseware*	2 years	2 years
Exam Voucher**(non-RPS)	1 year	1 year
Exam Retakes*** (non-RPS)	1	x
Ethical Hacking Videos*	1 year	1 year
EC-Council Labs*	6 months	x
C|EH Engage*	1 year	x
Global C|EH Challenge*	1 year	x
C|EH Practical****	1 year	x

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

*Ważny od daty aktywacji.

** Kupon egzaminacyjny - ważny przez 1 rok od daty złożenia oceny po szkoleniu (non-RPS Remote Proctor Services)

*** Maksymalnie 1 ponowne podejście do egzaminu dozwolone zgodnie z polityką ponownego podejścia do egzaminu. Polityka ponownego podejścia do egzaminu https://cert.eccouncil.org/exam-retake-policy.html

**** Panel CEH Practical zostanie aktywowany po kliknięciu “OK Proceed” w panelu egzaminacyjnym.

Pakiet - Warunki:

1. Ponowne podejścia do egzaminu będą regulowane zgodnie z polityką ponownego podejścia do egzaminu. Więcej szczegółów można znaleźć w polityce ponownego podejścia do egzaminu https://cert.eccouncil.org/exam-retake-policy.html
2. Ponowne podejścia do egzaminu dotyczyć tylko egzaminu CEH (MCQ), a nie CEH (Practical) i nie może to być zamienione.
3. Maksymalnie 1 ponowne podejście do egzaminu jest dozwolone w okresie 1 roku dla pakietu CEH Elite.
4. Obniżenie pakietu z CEH Elite do innego nie jest dozwolone.
5. Aktywowany zestaw CEH v13 (Lite) nie może być zaktualizowany do wersji CEH Elite.
6. Pakiety sprzedane raz są bezzwrotne.
7. W pakiecie CEH Elite dostępnych jest 10 kursów wideo dotyczących etycznego hakowania.
8. Wszystkie komponenty pakietu zostaną automatycznie aktywowane po jednokrotnym wykorzystaniu kodu.
9. Globalne CEH Challenge i CEH Engage nie mogą być kupowane osobno jako samodzielne komponenty.
10. Żadne dwie oferty nie mogą być łączone ani wymieniane na inne produkty/oferty.

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001