

Certified Ethical Hacker

CEHv.13 AI

Firma EC-Council, by sprostać rosnącemu zapotrzebowaniu na nowe umiejętności i wiedzę o cyberbezpieczeństwie, opracowała szkolenie Certified Ethical Hacker. Niekonwencjonalne podejście do myślenia o infrastrukturze firmowej z punktu widzenia intruza jest niezwykle efektywnym mechanizmem nauczania, który otwiera oczy na wiele często zaniedbywanych obszarów naszej pracy.

Ekskluzywny program nauczania CEH Elite (Learn | Certify | Engage | Compete) przygotowuje uczestników do certyfikacji. Ten 4-częściowy program nauczania daje uczestnikom możliwość przeprowadzenia pełnej symulacji etycznego hakowania od początku do końca na przykładzie emulowanej organizacji.

Rywalizując ze specjalistami na całym świecie, otrzymasz roczny dostęp do 12 wyzwań CTF (Capture The Flag), z których każde trwa 4 godziny.

Doskonaląc umiejętności, będziesz na bieżąco z najnowszymi trendami w obszarze sztucznej inteligencji.

Co nowego w wersji CEHv13 AI?

- 1. Oparty na sztucznej inteligencji framework**
- 2. O 40% większa efektywność.**
 - poznasz techniki napędzane przez sztuczną inteligencję, aby zwiększyć efektywność obrony cybernetycznej o 40%, jednocześnie usprawniając przepływy pracy.
- 3. 2x większa produktywność.**
 - zaawansowane wykrywanie zagrożeń, ulepszone podejmowanie decyzji, adaptacyjne uczenie się, ulepszona sprawozdawczość i automatyzacja powtarzalnych zadań.

4. **Profesjoniści z dziedziny cyberbezpieczeństwa mogą doskonalić swoje umiejętności w realistycznych scenariuszach dzięki praktycznym laboratoriom.**

- Uczestnicy doświadczą 220+ praktycznych laboratoriów, 550 technik ataków oraz ponad 4000 narzędzi do hakowania i zabezpieczeń.

W nowej wersji CEHv13 AI szczególny nacisk położono na integrację AI w procesie wykrywania, analizy, automatyzacji oraz reagowania na zagrożenia, zwiększając tym samym skuteczność i produktywność działań defensywnych.

Certyfikat CEH jest jednym z najbardziej pożądanych na rynku pracy i pomaga zwiększyć szanse zatrudnienia na stanowiskach związanych z cyberbezpieczeństwem na całym świecie.

Sprawdź swoją wiedzę z zakresu:

- [CompTIA CySA+](#)
- [CompTIA Security+](#)
- [CompTIA Network+](#)
- [OSINT - Biały Wywiad, czyli jak dotrzeć do cennych informacji](#)
- [CEH - Certified Ethical Hacker](#)
- [ECIH - Certified Incident Handler](#)
- [Testy penetracyjne](#)



Odbiorcy szkolenia

Szkolenie przeznaczone jest dla specjalistów odpowiedzialnych za bezpieczeństwo systemów, aplikacji, sieci i danych w organizacji, a także dla osób, które chcą rozpocząć lub rozwinąć karierę w obszarze cyberbezpieczeństwa. W szczególności są to:

- Administratorzy sieci i systemów, specjaliści IT odpowiedzialni za infrastrukturę techniczną i jej zabezpieczenia.
- Inżynierowie bezpieczeństwa, pentesterzy i analitycy SOC, którzy chcą ugruntować i poszerzyć swoją wiedzę o najnowsze narzędzia i techniki.
- Audytorzy IT i osoby odpowiedzialne za compliance, którzy muszą znać wektory ataków i techniki wykrywania luk bezpieczeństwa.
- Zespoły techniczne w organizacjach objętych regulacjami NIS2, potrzebujące praktycznej wiedzy na

temat zabezpieczania kluczowej infrastruktury.

- Osoby nietechniczne z działów zarządzania ryzykiem i IT, które chcą zrozumieć sposoby działania hakerów i podnieść świadomość w zakresie zagrożeń.

□ Uwaga: Ze względu na intensywny charakter szkolenia, osoby spoza branży bezpieczeństwa IT mogą potraktować kurs jako wprowadzenie do zagrożeń i metod ataków – nie jest jednak wymagane doświadczenie eksperckie, a praktyka oparta na labach ułatwia przyswajanie wiedzy. Część ćwiczeń i materiału zawartego w szkoleniu jest przeznaczona również do pracy własnej.



Korzyści

Celem pracy etycznych hakerów jest identyfikacja słabych punktów organizacji oraz pomaganie w znalezieniu skutecznej metody obrony przed atakami na firmowe systemy. Uczestnicy dokonują kontrolowanych włamań do systemu „ofiary” i zdobywają praktyczne umiejętności efektywnej ochrony sieci. Podczas gdy konwencjonalne środki bezpieczeństwa są niezbędne, ważne jest, aby uzyskać perspektywę ludzi, którzy mogą potencjalnie zagrozić systemom.

W ramach szkolenia uczestnicy otrzymują voucher na egzamin CEH weryfikujący zdobytą wiedzę i umiejętności.

Uczestnicy szkolenia nauczą się:

- definiować i charakteryzować najważniejsze techniki ataków stosowanych przez hakerów,
- przeprowadzać rekonesans dotyczący własnej firmy czy konkurencji,
- skanować, testować i przełamywać zabezpieczenia systemów,
- identyfikować i analizować podatności w organizacji,
- rozpoznawać i zapobiegać metodom eskalacji uprawnień w systemach,
- tworzyć lepsze polityki na urządzeniach IDS/IPS dotyczące wykrywania włamań,
- rozpoznawać socjotechniki wykorzystywane przez przestępców,
- generować wirusy, hakować urządzenia mobilne, smartfony,
- analizować złośliwe oprogramowanie,
- identyfikować potencjał zagrożeń płynących z "Internetu Rzeczy" (IoT) i jak się przed nimi zabezpieczyć,
- określić wyzwania dla sieci przemysłowych i wpływ cyberbezpieczeństwa na koncepcje OT (Operational Technology),
- charakteryzować najważniejsze elementy systemów kontenerowych (Docker, Kubernetes),
- weryfikować bezpieczeństwo rozwiązań chmurowych takich jak AWS,
- rozpoznawać subtelne różnice między backdoor'ami, trojanami oraz innymi zagrożeniami,
- docelowo, będą mogli skuteczniej uświadamiać pracowników firmy w kwestiach bezpieczeństwa informacji,

Nadchodzi nowa ulepszona v13 z dodatkowymi elementami sztucznej inteligencji, dzięki temu uczestnicy zdobędą:

- Dogłębną wiedzę na temat metodologii i praktyk etycznego hackingu, wzbogaconą o techniki AI

- Umiejętności integracji AI w różnych fazach etycznego hackingu: rozpoznanie, skanowanie, uzyskiwanie dostępu, utrzymywanie dostępu i zacieranie śladów
- Techniki AI do automatyzacji zadań, zwiększania efektywności oraz wykrywania zaawansowanych zagrożeń, które wykraczają poza tradycyjne metody
- Narzędzia, które wykorzystują AI do proaktywnego poszukiwania zagrożeń, wykrywania anomalii oraz analizy predykcyjnej w celu zapobiegania cyberatakam



Program szkolenia

1. Wprowadzenie do „Etycznego Hackingu”
2. Footprinting i Rekonesans - wstępne zbieranie informacji o celu ataku
3. Skanowanie sieci - identyfikacja systemów, portów, usług działających w sieci
4. Enumeracja - aktywne odpytywanie usług/systemów w celu rozpoznania słabych punktów w infrastrukturze
5. Analiza podatności - omówienie narzędzi do wykonywania skanowania oraz kryteriów ich doboru
6. Włamywanie się do systemów („Hakowanie” systemów)
7. Zagrożenia malware - rodzaje niebezpiecznego oprogramowania i mechanizmy działania
8. Podśluchiwanie (Sniffing) sieci - przechwytywanie danych
9. Socjotechniki (Inżynieria społeczna)
10. Ataki na odmowę dostępu do usługi (Denial-of-Service)
11. Przechwytywanie sesji - przejęcie komunikacji między ofiarą a systemem docelowym
12. Omijanie systemów IDS, firewall’i, honeypot’ów
13. Atakowanie serwerów webowych
14. Atakowanie aplikacji webowych
15. SQL Injection - ataki z wykorzystaniem braku odpowiedniego filtrowania zapytań baz danych SQL
16. Włamywanie się do sieci bezprzewodowych
17. Hakowanie platform i urządzeń mobilnych
18. Hakowanie "Internetu Rzeczy" oraz "Technologii Operacyjnych" (IoT i OT)
19. Konceptje i bezpieczeństwo rozwiązań chmurowych (cloud computing)
20. Kryptografia



Oczekiwane przygotowanie uczestnika

Wymagana podstawowa znajomość systemów operacyjnych Windows oraz Linux.

Zalecane przynajmniej dwuletnie doświadczenie w branży IT, znajomość protokołu TCP / IP (w tym usług takich jak DNS czy DHCP, znajomość koncepcji adresacji IP, routingu, przełączania w sieciach LAN).



Szkolenie obejmuje

- 5 dni pracy z trenerem
- Nadzór trenera

Poniższa tabela zawiera wykaz komponentów, które otrzymuje uczestnik w zależności od zakupionej wersji szkolenia.

Usługi dodatkowe wymagają aktywacji w pierwszym dniu szkolenia. Ważność całości pakietu liczona od dnia rozpoczęcia kursu – wyjątkiem są laboratoria, których ważność wynosi 6 miesięcy.



Język

- Szkolenie: polski
- Materiały: angielski

Czas trwania

5 dni / 40 godzin

Metoda egzaminacyjna

Do egzaminu **Knowledge-Based Exam** 312-50 (ECC Exam)

można przystąpić w autoryzowanych ośrodkach egzaminacyjnych EC-Council.

Tytuł – Certified Ethical Hacker

Format testu: Pytania wielokrotnego wyboru

Ilość pytań – 125

Czas trwania – 4 godz.

Uwaga: zdając egzamin CEH w formule online z tzw. ochroną zdalną, obowiązuje dodatkowa opłata 100 USD netto.

Koszt obejmuje wynajęcie osoby nadzorującej egzamin (tzw. proktora), zakupu dokonujemy indywidualnie na stronie vendora: <https://store.eccouncil.org/product/voucher-upgrade-rps-to-vue/>

Dodatkowo zakupując wersję szkolenia w pakiecie Elite:

Practical Exam

Format testu: Pytania oparte na prawdziwych scenariuszach

Ilość pytań - 20 scenariuszy

Czas trwania - 6 godz.