Szkolenie: EC-Council

# CPENT - Certified Penetration Testing Professional v2

## DOSTĘPNE TERMINY

2026-05-04 | 5 dni | Kraków / Virtual Classroom
2026-05-11 | 5 dni | Kraków / Wirtualna sala
2026-06-08 | 5 dni | Warszawa / Virtual Classroom
2026-06-15 | 5 dni | Warszawa / Wirtualna sala
2026-07-13 | 5 dni | Kraków / Wirtualna sala
2026-08-10 | 5 dni | Warszawa / Wirtualna sala

## Cel szkolenia:

Zdobądź zaawansowane umiejętności pentestera dzięki szkoleniu CPENT – Certified Penetration Testing Professional v2 – CPENT AI . Program Certified Penetration Testing Professional (CPENT AI ) to kompleksowe szkolenie z zakresu testów penetracyjnych, które umożliwia opanowanie technik penetracyjnych w środowiskach zarówno małych, średnich, jak i dużych przedsiębiorstw. Nauczysz się oceniać ryzyko włamań oraz opracowywać przejrzyste i praktyczne raporty. Poznasz, jak precyzyjnie określać zakres prac, analizować architekturę, szacować nakład pracy oraz prezentować wyniki. CPENT AI łączy naukę pod kierunkiem instruktora z praktycznymi ćwiczeniami, bazując na realistycznych scenariuszach obejmujących systemy IoT, segmentowane sieci oraz zaawansowane zabezpieczenia – każde zagadnienie poparte jest praktycznym wyzwaniem. Zyskasz specjalistyczną wiedzę niezbędną do tworzenia własnych narzędzi, przeprowadzania zaawansowanej eksploatacji binarnej, stosowania techniki double pivoting, personalizacji skryptów oraz pisania własnych exploitów, aby uzyskać dostęp do najbardziej ukrytych części sieci.

Umiejętności, które zdobędziesz dzięki szkoleniu CPENT[AI]:

- Zdobędziesz kompleksową wiedzę na temat procesów, procedur, technologii i workflow w SOC (Security Operations Center).
- Poznasz podstawy testów penetracyjnych, w tym ich cele, metodyki, ramy oraz znaczenie w strategii bezpieczeństwa organizacji.
- Dowiesz się, jak określać zakres testów penetracyjnych, definiować cele, skutecznie komunikować się z interesariuszami oraz przestrzegać granic prawnych i etycznych.
- Poznasz techniki OSINT do gromadzenia użytecznych informacji oraz nauczysz się identyfikować, mapować i analizować powierzchnię ataku organizacji.
- Opanujesz sztukę wykorzystywania socjotechniki w przełamywaniu ludzi oraz poznasz środki zapobiegawcze minimalizujące takie ryzyka.
- Wykształcisz techniki testowania aplikacji webowych pod kątem podatności takich jak SQL



Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 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

injection, XSS czy błędy uwierzytelniania i nauczysz się je wykorzystywać oraz eliminować.

- Zrozumiesz ocenę bezpieczeństwa API poprzez testowanie punktów końcowych, wykorzystywanie błędów konfiguracyjnych oraz identyfikację słabości w JSON Web Tokens (JWT).
- Poznasz zaawansowane techniki omijania firewalli, systemów wykrywania włamań (IDS), routerów, switchy i innych zabezpieczeń.
- Poznasz metody eksploatacji podatności w systemach Windows oraz metody przeprowadzania eskalacji uprawnień w celu uzyskania wyższego poziomu dostępu.
- Dowiesz się, jak testować i wykorzystywać podatności w środowiskach Active Directory poprzez identyfikację błędów konfiguracyjnych i luk bezpieczeństwa.
- Opanujesz techniki eksploatacji systemów Linux oraz eskalacji uprawnień, a także poznasz najczęstsze podatności i konfiguracje.
- Poznasz techniki reverse engineeringu, fuzzingu oraz eksploatacji binarnej w celu identyfikacji i wykorzystania słabości w oprogramowaniu i aplikacjach.
- Zdobędziesz techniki poruszania się po sieciach wewnętrznych, uzyskiwania dostępu do kolejnych systemów i pivotowania do krytycznych zasobów podczas testów penetracyjnych.
- Nauczysz się znajdować i wykorzystywać podatności w urządzeniach i ekosystemach IoT.
- Dowiesz się, jak przygotować profesjonalne raporty z testów penetracyjnych, skutecznie komunikować wnioski oraz przedstawiać rekomendacje do wdrożenia po testach.

Umiejętności AI, które zdobędziesz dzięki szkoleniu CPENT$^{AI}$:

- Zbieranie i analiza informacji z otwartych źródeł (OSINT) na potrzeby rekonesansu.
- Automatyzacja procesu skanowania sieci poprzez generowanie skryptów i komend za pomocą narzędzi AI.
- Identyfikacja potencjalnych powierzchni ataku.
- Identyfikacja i priorytetyzacja podatności w sieciach, aplikacjach i systemach.
- Przeprowadzanie różnorodnych ataków na sieci, aplikacje i systemy.
- Wykonywanie ataków socjotechnicznych przy użyciu narzędzi AI.
- Stosowanie narzędzi AI do ataków brute force i słownikowych w celu efektywnego łamania haseł.
- Przeprowadzanie enumeracji Active Directory.
- Wykorzystanie AI w reverse engineeringu do zrozumienia struktury binarnej i przepływu aplikacji.
- Automatyzacja procesów fuzzingu z użyciem AI w celu wykrywania błędów i podatności w oprogramowaniu.

Szkolenie CPENT $^{AI}$ jest dedykowane dla:

- Każdy specjalista ds. cyberbezpieczeństwa, który chce poszerzyć swoją wiedzę w zakresie



Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 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

bezpieczeństwa defensywnego.

- Penetration Tester
- Penetration Testing Consultant
- Penetration Testing Engineer
- Security Penetration Testing Consultant / Architect
- Vulnerability Assessment and Penetration Testing (VAPT) Analyst / Engineer
- QA Security Tester
- Web Application Penetration Tester
- Vulnerability Assessment Specialist
- Red Team - VAPT Security Consultant
- Penetration Test Lead
- Network Penetration Testing Engineer
- Director of Technical Advisor
- Senior Manual Ethical Hacker
- Senior API Security Vulnerability Analyst
- Application Security Engineer (Penetration Tester)
- Senior Web Application Security Specialist
- Senior Red Team Operator
- Cyber Threat Operator
- Computer Exploitation Test Engineer (Penetration Tester)
- Security Vulnerability Management Lead
- Security Lit - AI/ML Security Engineer
- AI Cyber Security Advisory Engineer
- Cyber Security Engineer (Generative AI)

*Każdy uczestnik autoryzowanego szkolenia szkolenia CPENT - Certified Penetration Testing Professional v2 realizowanego w Compendium CE, otrzymuje darmowy voucher egzaminacyjny CPENT v2.*

## Plan szkolenia:

- Moduł 1 - Introduction to Penetration Testing and Methodologies
  - Zasady i cele testów penetracyjnych
  - Metodyki i frameworki stosowane w pentestingu
  - Najlepsze praktyki i wytyczne dla testów penetracyjnych



Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 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

- Rola sztucznej inteligencji w procesie pentestingu
- Znaczenie testów penetracyjnych w kontekście zgodności z przepisami, regulacjami i standardami
- Kluczowe zagadnienia
  - Penetration Testing, proces pentestingu, metodyki i frameworki (w tym MITRE ATT&CK), cechy skutecznego testu penetracyjnego, AI-Driven Penetration Testing, narzędzia oparte na sztucznej inteligencji, testy zgodności (Compliance-Driven Penetration Testing), rola AI i uczenia maszynowego w testach zgodności.

- Moduł 2 - Zakres i zaangażowanie w testy penetracyjne
  - Działania przygotowawcze przed rozpoczęciem testów penetracyjnych
  - Kluczowe elementy odpowiedzi na zapytania ofertowe (RFP) dotyczące testów penetracyjnych
  - Opracowanie skutecznych zasad współpracy (Rules of Engagement – ROE)
  - Aspekty prawne i regulacyjne istotne dla testów penetracyjnych
  - Zasoby i narzędzia niezbędne do skutecznego przeprowadzenia testów
  - Strategie efektywnego zarządzania rozszerzaniem zakresu (scope creep)
  - Kluczowe zagadnienia
    - Przygotowanie propozycji ofertowej, zasady współpracy (ROE), tworzenie kontraktów na testy penetracyjne, reguły postępowania, umowy o poufności (NDA), kwestie odpowiedzialności, listy intencyjne, spotkania rozpoczynające projekt (kickoff), zakres prac (Statement of Work), przygotowanie planu testów, umowy dotyczące wykorzystania danych, briefing misji oraz zarządzanie rozszerzaniem zakresu.

- Moduł 3 - Open-Source Intelligence (OSINT)
  - Zbieranie informacji OSINT dotyczących nazwy domeny celu
  - Pozyskiwanie danych o organizacji docelowej z sieci
  - Wykonywanie OSINT na pracownikach celu
  - Wykorzystanie narzędzi automatyzujących OSINT
  - Mapowanie powierzchni ataku
  - Laboratoria
    - Zbieranie OSINT dotyczącego domeny, zasobów sieciowych i pracowników celu
    - Wykorzystanie narzędzi do automatyzacji OSINT
    - Identyfikacja i mapowanie powierzchni ataku
  - Kluczowe zagadnienia
    - Wyszukiwanie domen i subdomen, zapytania WHOIS, rekordy DNS, odwrotne wyszukiwanie DNS, transfer stref DNS, zaawansowane wyszukiwania w sieci (operatory), Google Dorking, footprinting z użyciem Shodan, pozyskiwanie adresów e-mail, wyszukiwanie osób w serwisach online, automatyzacja procesu OSINT przy użyciu narzędzi i frameworków, mapowanie powierzchni ataku, analiza traceroute, skanowanie sieci celu, wykrywanie aktywnych hostów, skanowanie portów,



Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 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

pobieranie banerów systemowych (OS Banner Grabbing) oraz fingerprinting usług.

- Moduł 4 - Testy penetracyjne z wykorzystaniem inżynierii społecznej
  - Podstawowe koncepcje testów penetracyjnych opartych na inżynierii społecznej
  - Testy inżynierii społecznej realizowane zdalnie (off-site)
  - Testy inżynierii społecznej realizowane na miejscu (on-site)
  - Dokumentowanie wyników wraz z rekomendacjami dotyczącymi środków zaradczych
  - Laboratoria
    - Przechwytywanie danych uwierzytelniających przy użyciu Social-Engineer Toolkit (SET)
  - Kluczowe zagadnienia
    - Proces testów penetracyjnych opartych na inżynierii społecznej, testy off-site, phishing, inżynieria społeczna przez telefon, wykorzystanie AI i uczenia maszynowego w inżynierii społecznej, testy on-site oraz środki zaradcze przeciwko atakom socjotechnicznym.
- Moduł 5 - Testy penetracyjne aplikacji webowych
  - Techniki footprintingu i enumeracji aplikacji webowych
  - Metody skanowania podatności w aplikacjach webowych
  - Testowanie podatności w konfiguracji i wdrożeniu aplikacji
  - Ocena mechanizmów zarządzania tożsamością, uwierzytelniania i autoryzacji
  - Analiza bezpieczeństwa zarządzania sesjami
  - Ocena mechanizmów walidacji danych wejściowych
  - Wykrywanie i eksploatacja podatności typu SQL Injection
  - Techniki identyfikacji i testowania podatności typu Injection
  - Eksploatacja podatności związanych z niewłaściwą obsługą błędów
  - Identyfikacja słabych mechanizmów kryptograficznych
  - Testowanie błędów logiki biznesowej w aplikacjach webowych
  - Ocena podatności po stronie klienta
  - Laboratoria
    - Wykonanie footprintingu strony internetowej
    - Przeprowadzenie skanowania podatności aplikacji webowej z wykorzystaniem AI
    - Realizacja różnych ataków na docelową aplikację webową
  - Kluczowe zagadnienia
    - Framework OWASP do testów penetracyjnych, footprinting stron, web spidering, mirroring stron, wykrywanie usług HTTP, pobieranie banerów serwera, testowanie domyślnych danych uwierzytelniających, enumeracja katalogów serwera WWW, ocena podatności aplikacji webowych, fuzzing aplikacji webowych, brute forcing katalogów, skanowanie podatności, testowanie obsługi rozszerzeń plików, testowanie kopii zapasowych i nieużywanych plików, enumeracja nazw użytkowników, ataki na autoryzację, niebezpieczne metody kontroli dostępu,



Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 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

sniffing tokenów sesji, przejęcie sesji, Cross-Site Request Forgery (XSRF), manipulacja parametrami URL, SQL Injection, LDAP Injection, niewłaściwa obsługa błędów, błędy logiki, Frame Injection.

- Moduł 6 - Testy penetracyjne API i JSON Web Token (JWT)
  - Techniki i narzędzia do przeprowadzania rekonesansu API
  - Testowanie API pod kątem podatności w uwierzytelnianiu i autoryzacji
  - Ocena bezpieczeństwa tokenów JSON Web Token (JWT)
  - Testowanie API pod kątem walidacji danych wejściowych i podatności typu Injection
  - Identyfikacja i eksploatacja podatności wynikających z błędnej konfiguracji zabezpieczeń
  - Testowanie API pod kątem ograniczeń szybkości (Rate Limiting) i ataków typu DoS
  - Ocena bezpieczeństwa implementacji GraphQL
  - Testowanie API pod kątem błędów logiki biznesowej i zarządzania sesjami
  - Laboratoria
    - Wykonanie rekonesansu API z wykorzystaniem AI
    - Skanowanie i identyfikacja podatności w API
    - Eksploatacja różnych podatności w celu uzyskania informacji o aplikacji docelowej
  - Kluczowe zagadnienia
    - Rekonesans API, testy API pod kątem błędów uwierzytelniania, testy API dla uprawnień na poziomie obiektów (BOLA), testy JWT, podatności SQL Injection w API, testy API pod kątem Cross-Site Scripting (XSS), fuzzing danych wejściowych API, skanowanie podatności API, nadużycia związane z konsumpcją zasobów API, ataki związane z ograniczeniami szybkości i throttlingiem, problemy bezpieczeństwa GraphQL, obchodzenie przepływów pracy w API, przejęcie sesji w API.
- Moduł 7 - Techniki omijania zabezpieczeń perymetrycznych
  - Techniki oceny implementacji zabezpieczeń firewalli
  - Techniki oceny implementacji zabezpieczeń systemów IDS (Intrusion Detection System)
  - Metody oceny bezpieczeństwa routerów
  - Metody oceny bezpieczeństwa przełączników (switches)
  - Laboratoria
    - Identyfikacja i obejście firewalla
    - Omijanie zabezpieczeń perymetrycznych z wykorzystaniem Social-Engineer Toolkit (SET)
    - Fingerprinting zapory aplikacji webowych (WAF)
  - Kluczowe zagadnienia
    - Testowanie firewalli, lokalizacja firewalli, enumeracja list kontroli dostępu (ACL) w firewallach, skanowanie firewalli pod kątem podatności, omijanie firewalli, testy penetracyjne IDS, techniki omijania systemów IDS, testowanie IDS różnymi metodami, omijanie IDS, problemy związane z testowaniem routerów, skanowanie portów routera, testowanie błędnych konfiguracji routerów, identyfikacja błędnych konfiguracji zabezpieczeń w switchach, testowanie wydajności OSPF, audyt



Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 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

bezpieczeństwa routerów i switchy.

- Moduł 8 - Eksploatacja systemów Windows i eskalacja uprawnień
  - Metodyka testów penetracyjnych systemów Windows
  - Techniki rekonesansu na systemach Windows
  - Metody oceny podatności i weryfikacji exploitów
  - Sposoby uzyskania początkowego dostępu do systemów Windows
  - Techniki enumeracji z uprawnieniami użytkownika
  - Metody eskalacji uprawnień
  - Działania po eksploatacji (post-exploitation)
  - Laboratoria
    - Eksploatacja podatności systemu Windows
    - Eksploatacja i eskalacja uprawnień w systemie Windows
    - Uzyskanie dostępu do systemu zdalnego
    - Eksploatacja podatności typu Buffer Overflow na maszynie Windows
  - Kluczowe zagadnienia
    - Rekonesans w systemach Windows, skanowanie podatności Windows, uzyskiwanie dostępu do systemu Windows, skanowanie podatności i sugestie exploitów z wykorzystaniem AI, łamanie haseł, uzyskiwanie dostępu do Windows przez Remote Shell, eksploatacja podatności typu Buffer Overflow w Windows, techniki post-exploitation z użyciem Meterpreter, eskalacja uprawnień, obejście UAC, unikanie wykrycia przez antywirusy, wyłączanie Windows Defender, konfiguracja backdoora przy starcie systemu, unikanie detekcji antywirusowej.
- Moduł 9 - Testy penetracyjne Active Directory
  - Architektura i kluczowe komponenty Active Directory
  - Techniki rekonesansu Active Directory
  - Metody enumeracji Active Directory
  - Eksploatacja zidentyfikowanych podatności Active Directory
  - Rola sztucznej inteligencji w strategiach testów penetracyjnych AD
  - Laboratoria
    - Analiza i eksploracja środowiska Active Directory
    - Wykonywanie enumeracji Active Directory
    - Realizacja poziomej eskalacji uprawnień i ruchu lateralnego
    - Pobieranie buforowanych danych uwierzytelniających Active Directory
  - Kluczowe zagadnienia
    - Podstawy Active Directory, komponenty AD, techniki rekonesansu, enumeracja Active Directory, interfejsy usług AD (ADSI), narzędzia do enumeracji AD, ataki typu Password Spraying, usługi certyfikatów Active Directory (AD CS), enumeracja użytkowników serwera Exchange, eksploatacja serwera Exchange, ekstrakcja hashy haseł, łamanie hashy NTLM, eksploatacja Active Directory oraz enumeracja



Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 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

AD z wykorzystaniem AI.

- Moduł 10 - Eksploatacja systemów Linux i eskalacja uprawnień
  - Metodyki eksploatacji i testów penetracyjnych systemów Linux
  - Techniki rekonesansu i skanowania podatności w systemach Linux
  - Metody uzyskania początkowego dostępu do systemów Linux
  - Techniki eskalacji uprawnień w systemach Linux
  - Laboratoria
    - Wykonanie rekonesansu i oceny podatności w systemie Linux
    - Uzyskanie dostępu i przeprowadzenie enumeracji
    - Identyfikacja błędnych konfiguracji w celu eskalacji uprawnień
  - Kluczowe zagadnienia
    - Testy penetracyjne systemów Linux, skanowanie podatności Linux, techniki eskalacji uprawnień, rekonesans w systemach Linux, metody enumeracji, eksploatacja błędnych konfiguracji, łamanie haseł, dostęp przez zdalną powłokę (Remote Shell), eksploatacja podatności typu Buffer Overflow w Linux, strategie post-exploitation oraz mechanizmy utrzymywania dostępu (Persistence).
- Moduł 11 - Inżynieria wsteczna, fuzzing i eksploatacja binarna
  - Koncepcje i metody analizy binariów Linux
  - Metody analizy binariów Windows
  - Ataki typu Buffer Overflow i metody ich eksploatacji
  - Zasady, metody i narzędzia do fuzzingu aplikacji
  - Laboratoria
    - Analiza binariów
    - Poznanie metodologii analizy binariów
    - Pisanie kodu exploita
    - Inżynieria wsteczna binariów
    - Identyfikacja i debugowanie przepełnień stosu (Stack Buffer Overflow)
    - Fuzzing aplikacji
  - Kluczowe zagadnienia
    - Instrukcje maszynowe, asembler 32-bitowy, binaria ELF, instrukcje IA-32 w testach penetracyjnych, metodologia analizy binariów, framework Capstone, analiza statyczna, analiza dynamiczna, programy w x86 C, przepełnienie bufora, przepełnienie sterty (Heap Overflow), exploity korupcji pamięci, kompilacja krzyżowa binariów, techniki fuzzingu, etapy fuzzingu, rodzaje fuzzera, debugowanie, narzędzia do fuzzingu, tworzenie własnych fuzzerów.
- Moduł 12 - Ruch lateralny i pivoting
  - Zaawansowane techniki ruchu lateralnego w sieciach
  - Zaawansowane metody pivotingu i tunelowania w celu utrzymania dostępu
  - Laboratoria



Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 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

        - Wykonanie pivotingu
        - Realizacja tunelowania DNS i HTTP
    - Kluczowe zagadnienia
        - Strategie ruchu lateralnego, ataki Pass-the-Hash (PtH), ataki Pass-the-Ticket (PtT), ataki Kerberos, Silver Ticket i Golden Ticket, Kerberoasting, wykorzystanie PsExec i Metasploit Framework do ruchu lateralnego, Windows Remote Management (WinRM) do ruchu lateralnego, łamanie RDP, techniki pivotingu i narzędzia, tunelowanie HTTP, tunelowanie DNS, tunelowanie ICMP, tunelowanie SSH oraz przekierowywanie portów (Port Forwarding).
- Moduł 13 - Testy penetracyjne IoT
    - Podstawowe koncepcje testów penetracyjnych IoT
    - Zbieranie informacji i mapowanie powierzchni ataku
    - Analiza firmware urządzeń IoT
    - Dogłębna analiza oprogramowania IoT
    - Ocena bezpieczeństwa sieci i protokołów IoT
    - Strategie poeksploatacyjne i techniki utrzymywania dostępu
    - Kompleksowe raporty z testów penetracyjnych
    - Laboratoria
        - Pozyskiwanie, ekstrakcja, analiza i emulacja firmware IoT
        - Badanie urządzeń IoT
    - Kluczowe zagadnienia
        - Testy penetracyjne IoT, OWASP Top 10 zagrożeń IoT, obszary powierzchni ataku IoT według OWASP, metodologia testów penetracyjnych IoT, identyfikacja urządzeń IoT, analiza firmware, ekstrakcja obrazu firmware, inżynieria wsteczna firmware, analiza statyczna i dynamiczna binariów, analiza oprogramowania IoT, testowanie bezpieczeństwa sieci i protokołów IoT, analiza ruchu sieciowego między urządzeniami, bramkami i serwerami, techniki eskalacji uprawnień w IoT, techniki ruchu lateralnego w sieciach IoT oraz przygotowanie raportu z testów penetracyjnych IoT.
- Moduł 14 - Tworzenie raportów i działania po testach
    - Cel i struktura raportu z testów penetracyjnych
    - Kluczowe elementy raportu z testów penetracyjnych
    - Etapy tworzenia raportu z testów penetracyjnych
    - Umiejętności niezbędne do skutecznego przygotowania raportu
    - Działania po zakończeniu testów w organizacji
    - Laboratoria
        - Generowanie raportów z testów penetracyjnych
    - Kluczowe zagadnienia
        - Cechy dobrego raportu z testów penetracyjnych, komponenty raportu, fazy tworzenia raportu, przygotowanie wersji roboczej, narzędzia do tworzenia



Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 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

raportów, dostarczanie raportu z testów penetracyjnych, przechowywanie raportu, niszczenie raportu, dokumentacja zatwierdzająca (sign-off), opracowanie i wdrożenie planu kopii zapasowych, prowadzenie szkoleń, ponowne testy i walidacja.

## Wymagania:

Zalecane jest:

- Minimum 2 lata doświadczenia w IT lub cyberbezpieczeństwie.
- Znajomość podstawowych zagadnień z zakresu sieci, systemów operacyjnych (Windows/Linux) oraz bezpieczeństwa.
- Posiadanie certyfikacji **CEH (Certified Ethical Hacker)** lub równoważnej wiedzy praktycznej.

## Poziom trudności

## Certyfikaty:

Uczestnicy szkolenia otrzymują certyfikat ukończenia szkolenia sygnowany przez EC-Council (ukończenie szkolenia). Kurs ten przygotowuje także do egzaminu certyfikacyjnego CPENT v2 (CPENT $^{AI}$).

Szczegóły egzaminu CPENT v2:

- Kod egzaminu: 312-39
- Czas trwania: 24 godziny lub do wyboru 2 sesje po 12 godzin każda
- Złożenie raportu: Raport z testów penetracyjnych należy przesłać w ciągu 7 dni od egzaminu
- Format egzaminu: 100% egzamin praktyczny
- Podwójna certyfikacja: Uzyskaj wynik powyżej 90% i otrzymaj dodatkowy certyfikat – Licensed Penetration Tester

*Każdy uczestnik autoryzowanego szkolenia szkolenia CPENT - Certified Penetration Testing Professional v2 realizowanego w Compendium CE, otrzymuje darmowy voucher egzaminacyjny CPENT v2.*



Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 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

## Prowadzący:

Certified EC-Council Instructor (CEI)

## Informacje dodatkowe:

Materiały szkoleniowe składają się z oficjalnego podręcznika EC-Council w wersji elektronicznej, dostępu do CPENT Cyber Range na okres 90 dni i labolatorium iLabs na 180 dni i vouchera egzaminacyjnego.



Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 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