kod szkolenia: CPENT AI / PL DL 5d NIS2

CPENT AI : Certified Penetration Testing Professional v2

Jest to pięciodniowy kurs, który oferuje uczestnikom kompleksowe zrozumienie koncepcji, terminologii i zasad stosowanych w profesjonalnych testach penetracyjnych. Obejmuje kluczowe koncepcje z opublikowanej przez EC-Council metodologii testów penetracyjnych, aby zapewnić kompleksowe, oparte na standardach podejście metodologiczne do dostarczania profesjonalnych testów penetracyjnych. CPENT AI skupia się na wykorzystaniu algorytmów sztucznej inteligencji na każdym etapie testu penetracyjnego. Wykorzystanie sztucznej inteligencji w pracy pentestera zwiększa produktywność i jakość wykonywanych testów. Po ukończeniu kursu uczestnik będzie wyposażony w odpowiednią wiedzę, aby przygotować się do egzaminu CPENT. CPENT w całości skupia się na praktyce. Pozwala zdobyć gruntowną praktykę dzięki wyzwaniom CTF, największej bibliotece ponad 100 laboratoriów.

Sprawdź, czy Twoja firma będzie objęta dyrektywą NIS2

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 skierowane jest do specjalistów bezpieczeństwa IT, którzy chcą pogłębić swoje kompetencje w zakresie ofensywnego bezpieczeństwa, a także do osób przygotowujących się do roli certyfikowanego pentestera. W szczególności:

- Inżynierów bezpieczeństwa IT, administratorów systemów i sieci, członków zespołów SOC.
- Pentesterów i red teamów, którzy chcą zdobyć formalną certyfikację i nauczyć się wykorzystywać AI w testach bezpieczeństwa.
- Audytorów i analityków bezpieczeństwa, którzy muszą rozumieć techniki ofensywne w celu lepszej oceny poziomu zabezpieczeń.
- Specjalistów IT, którzy planują wejść w obszar testów penetracyjnych i szukają szkolenia opartego na praktyce.
- Firm objętych regulacjami NIS2, które potrzebują wyspecjalizowanej kadry do przeprowadzania niezależnych testów bezpieczeństwa.

⚠ Szkolenie ma charakter zaawansowany. Podstawowa znajomość systemów Linux/Windows, protokołów sieciowych, oraz skryptów (PowerShell, Bash, Python) jest wymagana.

Korzyści

Ten kurs przygotuje uczestników do przystąpienia do egzaminu CPENT.
Po ukończeniu tego kursu będziesz w stanie uzyskać kompleksową, aktualną i dogłębną wiedzę w zakresie:

- wykorzystania narzędzi AI w procesie testów penetracyjnych
- technik testowania API oraz Java Web Token
- różnych podstawowych pojęć dotyczących testów penetracyjnych, w tym ich znaczenia, rodzajów, procesu, faz i metodologii.
- jak zainicjować, zaangażować i kontynuować zadanie testowania penetracyjnego.
- różnych umiejętności i technik zbierania informacji o celu z różnych publicznie dostępnych źródeł.
- jak wdrożyć kompleksową metodologię testów penetracyjnych w celu oceny ludzkich zachowań, które zwiększają podatność na potencjalne ataki socjotechniczne.
- jak wdrożyć kompleksową metodologię testów penetracyjnych do oceny sieci z perspektywy osób postronnych.
- jak wdrożyć kompleksową metodologię testów penetracyjnych do oceny bezpieczeństwa sieciowych urządzeń perymetrycznych, takich jak zapory ogniowe, systemy IDS, routery i przełączniki.
- jak wdrożyć kompleksową metodologię testów penetracyjnych do oceny bezpieczeństwa aplikacji internetowych i serwerów internetowych
- jak wdrożyć kompleksową metodologię testów penetracyjnych do oceny bezpieczeństwa infrastruktury bezprzewodowej

- jak ustanowić proces oceny urządzeń IoT, wyodrębniania oprogramowania układowego z urządzeń, montowania i uruchamiania obrazu oprogramowania układowego oraz badania exploitów IoT.
- wyzwań związanych z testowaniem ICS, SCADA, przeglądaniem protokołów sieciowych ICS/SCADA, analizowaniem ruchu sieciowego Modbus i modyfikowaniem danych sieciowych ICS/SCADA.
- jak wdrożyć kompleksową metodologię testów penetracyjnych do oceny bezpieczeństwa w systemach Windows oraz Linux
- jak wdrożyć kompleksową metodologię testów penetracyjnych do oceny bezpieczeństwa infrastruktury Active Directory
- jak wdrożyć kompleksową metodologię testów penetracyjnych do oceny bezpieczeństwa infrastruktury chmurowej
- exploitów binarnych, koncepcji przepełnienia bufora, przeglądania układu pamięci pod kątem stosów, analizowania pamięci i wyszukiwania słabych punktów, modyfikowania wykonania programu i obchodzenia podstawowych zabezpieczeń stosu.
- jak napisać kompleksowy raport z testów penetracyjnych dla docelowych odbiorców.

Certyfikat CPENT potwierdza wysokie kompetencje techniczne i daje przewagę w procesach rekrutacyjnych na stanowiska związane z cyberbezpieczeństwem.

Program szkolenia

1. Wprowadzenie do testów penetracyjnych
2. Zakres testów penetracyjnych – omówienie
3. Open Source Intelligence (OSINT)
4. Testy penetracyjne – inżynieria społeczna
5. Testy penetracyjne aplikacji internetowych
6. Testy penetracyjne API oraz Java Web Token
7. Techniki omijania ochrony obwodowej
8. Wykorzystanie luk w zabezpieczeniach systemu Windows i eskalacja uprawnień
9. Testy penetracyjne Active Directory
10. Wykorzystanie luk w zabezpieczeniach systemu Linux i eskalacja uprawnień
11. Inżynieria wsteczna, Fuzzing, analiza binarna
12. Ruch boczny oraz Pivoting
13. Testy penetracyjne IoT
14. Pisanie raportów i działania po testach

Self-Study

1. Podstawowe pojęcia dotyczące testów penetracyjnych
2. Metasploit Framework
3. Wprowadzenie do PowerShell, Bash, Python, Perl, Ruby
4. Testy penetracyjne sieci bezprzewodowych
5. Testy penetracyjne OT/SCADA

6. Testy penetracyjne – chmura
7. Testy penetracyjne baz danych
8. Testy penetracyjne urządzeń mobilnych

Oczekiwane przygotowanie uczestnika

Wymagana średniozaawansowana 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
- Kontakt ze społecznością
- Autoryzowany podręcznik w wersji elektronicznej
- Środowisko laboratoryjne – iLabs -180 dni
- voucher na egzamin

Metoda szkolenia

- wykład
- warsztaty

Język

- Szkolenie: polski
- Materiały: angielski

Metoda egzaminacyjna

CPENT jest egzaminem praktycznym w całości przeprowadzanym zdalnie w języku angielskim. Egzamin jest przez przeprowadzany w obecności osoby pełniącej role nadzorcy. Osoba przystępująca do egzaminu przez cały czas trwania egzaminu musi posiadać włączoną kamerę, mikrofon i udostępniony ekran.
Szkolenie zawiera voucher pozwalający na jedne podejście do egzaminu.

Certyfikat CPENT otrzymują kandydaci, którzy uzyskali 70% możliwych do uzyskania punktów, certyfikat LPT wymaga uzyskania co najmniej 90%.
Kandydaci, którzy uzyskają wynik powyżej 90%, zostaną uznani jako Penetration Testing Masters i zdobędą prestiżowy certyfikat LPT(Master)!

Czas trwania

5 dni / 35 godzin

Opis egzaminu

Egzamin można zdawać w formie jednej sesji 24 godzinnej lub dwóch sesjach po 12 godzin każda.