Możliwość dofinansowania

Szkolenie PEN-300 Evasion Techniques and Breaching Defenses - kompleksowy kurs e-learningowy

Numer usługi 2026/02/17/142469/3341323

7 870,77 PLN brutto
6 399,00 PLN netto
11,73 PLN brutto/h
9,54 PLN netto/h
261,33 PLN cena rynkowa

SOFTRONIC SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

4,3 / 5

201 ocen

Usługa szkoleniowa
zdalna
671:00 h
02.11.2026 do 31.01.2027

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie **PEN-300 Evasion Techniques and Breaching Defenses** to zaawansowany kurs testów penetracyjnych, który jest skierowany do doświadczonych specjalistów ds. bezpieczeństwa ofensywnego. Bazując na umiejętnościach zdobytych na PEN-200, PEN-300 koncentruje się na praktycznych technikach włamywania się i działania w obrębie zahartowanych celów oraz dojrzałych organizacji z ugruntowanymi programami bezpieczeństwa.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	5
Data zakończenia rekrutacji	20-10-2026
Forma prowadzenia usługi	zdalna
Podstawa uzyskania wpisu do BUR	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Celem kursu jest przygotowanie uczestników do wykonywania zaawansowanych technik ofensywnych obejmujących m.in. eksploatację po stronie klienta, inżynierię społeczną, kradzież danych uwierzytelniających, ruch boczny i eskalację uprawnień.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Opracowuje techniki ataków po stronie klienta.	omawia zasady przeprowadzania ataków po stronie klienta	Test teoretyczny z wynikiem generowanym automatycznie
	charakteryzuje podatności występujące w aplikacjach Microsoft Office i innych popularnych aplikacjach	Test teoretyczny z wynikiem generowanym automatycznie
	dobiera technikę ataku do specyfiki środowiska i celu testu	Test teoretyczny z wynikiem generowanym automatycznie
	omawia zasady działania mechanizmów wykrywania i blokowania złośliwego oprogramowania	Test teoretyczny z wynikiem generowanym automatycznie
Stosuje techniki omijania mechanizmów ochrony antywirusowej	charakteryzuje podstawowe i zaawansowane techniki unikania detekcji antywirusowej	Test teoretyczny z wynikiem generowanym automatycznie
	dobiera techniki i narzędzia omijania zabezpieczeń do badanego środowiska	Test teoretyczny z wynikiem generowanym automatycznie
Omija mechanizmy kontroli uruchamiania aplikacji	omawia zasady działania mechanizmów kontroli aplikacji w systemach Windows,	Test teoretyczny z wynikiem generowanym automatycznie
	charakteryzuje mechanizmy AppLocker i podobne rozwiązania,	Test teoretyczny z wynikiem generowanym automatycznie
	identyfikuje ograniczenia i potencjalne słabości konfiguracji mechanizmów kontroli aplikacji	Test teoretyczny z wynikiem generowanym automatycznie
	dobiera odpowiednią technikę obejścia zastosowanych ograniczeń,	Test teoretyczny z wynikiem generowanym automatycznie
	omawia zasady i mechanizmy wykorzystywane podczas lateral movement	Test teoretyczny z wynikiem generowanym automatycznie
Przeprowadza zaawansowane działania związane z przemieszczaniem się w środowisku sieciowym	charakteryzuje techniki przemieszczania się pomiędzy systemami Windows i Linux,	Test teoretyczny z wynikiem generowanym automatycznie
	identyfikuje dostępne mechanizmy uwierzytelniania i uprawnienia umożliwiające dostęp do kolejnych systemów,	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wykorzystuje podatności środowiska Active Directory.	omawia architekturę i mechanizmy bezpieczeństwa środowiska Active Directory,	Test teoretyczny z wynikiem generowanym automatycznie
	identyfikuje zależności pomiędzy kontami, grupami, uprawnieniami i zasobami domenowymi	Test teoretyczny z wynikiem generowanym automatycznie
	rozpoznaje potencjalne ścieżki eskalacji uprawnień w środowisku Active Directory,	Test teoretyczny z wynikiem generowanym automatycznie
Omija mechanizmy detekcji ruchu sieciowego	omawia zasady działania systemów IDS i IPS	Test teoretyczny z wynikiem generowanym automatycznie
	charakteryzuje mechanizmy wykrywania anomalii i sygnatur stosowane w systemach detekcji,	Test teoretyczny z wynikiem generowanym automatycznie
	dobiera techniki ograniczania możliwości wykrycia aktywności w sieci,	Test teoretyczny z wynikiem generowanym automatycznie
Wykorzystuje zaawansowane techniki eksploatacji Microsoft SQL Server i Active Directory.	omawia mechanizmy bezpieczeństwa i uwierzytelniania stosowane w Microsoft SQL Server	Test teoretyczny z wynikiem generowanym automatycznie
	identyfikuje potencjalne podatności i błędy konfiguracji usług bazodanowych,	Test teoretyczny z wynikiem generowanym automatycznie
	charakteryzuje zależności pomiędzy Microsoft SQL Server a środowiskiem domenowym,	Test teoretyczny z wynikiem generowanym automatycznie
	dobiera technikę eksploatacji do zidentyfikowanej podatności,	Test teoretyczny z wynikiem generowanym automatycznie
Wykorzystuje zaawansowane techniki programowania do opracowywania narzędzi testów bezpieczeństwa.	omawia zaawansowane koncepcje programowania wykorzystywane w testach penetracyjnych,	Test teoretyczny z wynikiem generowanym automatycznie
	charakteryzuje podstawowe mechanizmy Win32 API,	Test teoretyczny z wynikiem generowanym automatycznie
	dobiera funkcje Win32 API odpowiednie do realizacji określonego zadania,	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Kurs **PEN-300 Evasion Techniques and Breaching Defenses** to zaawansowany kurs testów penetracyjnych dla doświadczonych specjalistów ds. bezpieczeństwa ofensywnego. Bazując na umiejętnościach zdobytych na kursie PEN-200, kurs PEN-300 koncentruje się na praktycznych technikach włamywania się i działania w obrębie zahartowanych celów oraz dojrzałych organizacji z ugruntowanymi programami bezpieczeństwa. Kurs kładzie nacisk na praktyczne rozwijanie technik i narzędzi, zachęcając uczestników do wyjścia poza gotowe rozwiązania i tworzenia niestandardowych podejść, które sprawdzą się w walce z nowoczesnymi systemami obronnymi i ewoluującymi cyberzagrożeniami.

Szkolenie realizowane jest w formule **e-learningu asynchronicznego** (self-paced)

Uczestnik otrzymuje dostęp do indywidualnie wygenerowanego konta **na platformie OffSec** na okres **90 dni.** W tym czasie może korzystać z materiałów bez narzuconych terminów i godzin nauki, dostosowując tempo oraz harmonogram nauki do własnej dyspozycyjności.

Evasion Techniques and Breaching Defenses (PEN-300) e-learning

- 90 dni dostępu do kursu i laboratoriów praktycznych **na platformie OffSec**
- Jedno podejście do egzaminu certyfikacyjnego wliczone w cenę.
- Ponad 50 laboratoriów Proving Grounds Play – symulacje ataków w realistycznym środowisku.
- Bonusowy dostęp do kursu PEN-103, umożliwiający zdobycie dodatkowego certyfikatu.

Struktura szkolenia:

Kurs PEN-300 składa się **z ponad 20 modułów tematycznych**, obejmujących łącznie **671 godz.** Każdy moduł rozpoczyna się teorią, a następnie przechodzi do praktycznego zastosowania poprzez ćwiczenia i przykłady kodu. Wiele modułów zawiera instruktaże wideo dla osób uczących się wizualnie. Po ukończeniu modułów uczestnicy stosują zdobytą wiedzę w siedmiu laboratoriach typu Challenge Lab, które symulują złożone, realistyczne sytuacje i przygotowują ich do egzaminu OSEP.

Egzamin wymaga wykazania się umiejętnością identyfikowania, wykorzystywania i raportowania luk w zabezpieczeniach, w tym tworzenia własnych exploitów, zgodnie z profesjonalnymi standardami raportowania testów penetracyjnych..

Program szkolenia:

Teoria systemów operacyjnych i programowania

Poznanie zarządzania pamięcią, planowania procesów, systemów plików i innych kluczowych komponentów OS, aby zbudować solidne podstawy do rozumienia i wykorzystywania podatności.

Wykonywanie kodu po stronie klienta w Office

Wykorzystanie znanych luk w aplikacjach Microsoft Office do tworzenia złośliwych dokumentów uruchamiających kod na maszynie ofiary, umożliwiając nieautoryzowany dostęp i kontrolę.

Wykonywanie kodu po stronie klienta w Jscript

Eksploatacja Jscript w celu uruchamiania kodu, zdobywania nieautoryzowanego dostępu i kontroli nad systemami Windows.

Wstrzykiwanie procesów i migracja

Opanowanie technik ukrywania i utrzymywania dostępu poprzez wstrzykiwanie złośliwego kodu do prawidłowo działających procesów oraz migrację między procesami, aby uniknąć wykrycia.

Wprowadzenie do unikania antywirusa

Tworzenie złośliwego oprogramowania, które pozostaje niewykrywalne dzięki podstawowym technikom, takim jak zaciemnianie kodu i pakowanie.

Zaawansowane unikanie antywirusa

Wykorzystanie zaawansowanych metod, np. unikanie wykrywania sygnatur i heurystyki, aby tworzyć malware niewykrywalne przez rozbudowane systemy antywirusowe.

Whitelisting aplikacji

Omijanie zabezpieczeń ograniczających uruchamianie nieautoryzowanego oprogramowania.

Omijanie filtrów sieciowych

Uzyskiwanie dostępu do zastrzeżonych zasobów i sieci poprzez różne techniki omijania filtrów i zapór sieciowych.

Post-exploitation w Linuxie

Poruszanie się po systemie plików, zarządzanie kontami użytkowników, pozyskiwanie wrażliwych informacji oraz ustanawianie trwałych backdoorów na skompromitowanych systemach Linux.

Post-exploitation w Windows

Poruszanie się po systemie plików, zarządzanie kontami użytkowników, pozyskiwanie wrażliwych informacji oraz ustanawianie trwałych backdoorów na skompromitowanych systemach Windows.

Kiosk Breakouts

Przełamywanie ograniczeń środowisk kioskowych, takich jak bankomaty lub terminale POS, w celu przejęcia kontroli nad systemem operacyjnym.

Kredencjały Windows

Wydobywanie cennych danych uwierzytelniających, takich jak hasła i skróty, z systemów Windows.

Lateral Movement w Windows

Wykorzystanie relacji zaufania i podatności w usługach i protokołach (np. za pomocą PsExec, Mimikatz) do przemieszczania się po systemach w skompromitowanej sieci Windows.

Lateral Movement w Linux

Eksploatacja relacji zaufania i podatności w usługach i protokołach w celu przemieszczania się po systemach w skompromitowanej sieci Linux.

Ataki na Microsoft SQL

Atakowanie podatności w bazach Microsoft SQL Server w celu pozyskiwania wrażliwych danych, eskalacji uprawnień i kontroli nad systemami.

Eksploatacja Active Directory

Wykorzystanie podatności w Active Directory w celu kompromitacji domen w sieciach Windows.

Łączenie elementów

Łączenie wielu exploitów, technik i narzędzi w celu stworzenia złożonych, wieloetapowych ataków omijających różne poziomy zabezpieczeń.

Try Harder

Wykorzystywanie zdobytej wiedzy i umiejętności w wymagających, realistycznych scenariuszach z rozbudowaną infrastrukturą, wzmocnionymi zabezpieczeniami i realistycznymi wyzwaniami ataków..

Egzamin OffSec OSEP Standalone Exam

- - Certyfikacja OSEP — Egzamin praktyczny z cyberbezpieczeństwa na poziomie zaawansowanym, wymagający od uczestnika zastosowania zdobytej wiedzy w realistycznych scenariuszach korporacyjnych.
  - Czas trwania i nadzór — Egzamin trwa 48 godzin i jest nadzorowany zdalnie przez pracownika Offensive Security (proctor) w prywatnym połączeniu VPN, co zapewnia bezpieczeństwo i uczciwość testu.
  - Środowisko laboratoryjne — Kandydat pracuje w interaktywnym środowisku laboratoryjnym z rzeczywistymi systemami, gdzie identyfikuje, eksploatuje i raportuje prawdziwe podatności.

Zakres egzaminu:

- - Symulacja sieci korporacyjnej — Egzamin obejmuje duże, złożone środowisko sieciowe z wieloma maszynami do skompromitowania.
  - Wiele ścieżek ataku — Niektóre systemy wymagają wieloetapowej eksploatacji, podczas gdy inne są w pełni podatne na ataki zdalne.
  - Post-exploitation i lateral movement — Kandydat musi wykazać się umiejętnością przemieszczania się w sieci, utrzymania dostępu i łączenia exploitów w zaawansowane scenariusze.

Cel egzaminu — Sprawdzenie praktycznych umiejętności w zakresie:

- - identyfikacji i eksploatacji podatności w skomplikowanych środowiskach sieciowych,
  - utrzymania dostępu i przeprowadzania lateral movement,
  - stosowania wieloetapowych ataków i łączenia różnych technik,
  - raportowania wyników w sposób profesjonalny i zrozumiały.

Egzamin OSEP jest jednym z najbardziej wymagających certyfikatów zaawansowanego pentestingu, który potwierdza zdolność do przeprowadzania kompleksowych testów penetracyjnych w realistycznych, korporacyjnych środowiskach.

Cennik

Jeżeli korzystasz z dofinansowania i usługa stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego wraz z usługą lub dostawą towarów ściśle związaną z usługami kształcenia zawodowego lub przekwalifikowania zawodowego to możesz mieć możliwość skorzystania za zwolnienia z podatku VAT na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2024 r. o podatku od towarów i usług, jeśli usługa w całości jest finansowana ze środków publicznych lub § 3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień w przypadku, gdy usługa jest finansowana w co najmniej 70% ze środków publicznych.

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	7 870,77 PLN

Koszt przypadający na 1 uczestnika netto	6 399,00 PLN
Koszt osobogodziny brutto	11,73 PLN
Koszt osobogodziny netto	9,54 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	671:00

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Informacje o materiałach dla uczestników usługi

- **90 dni** dostępu do kursu (materiały do pobrania w pdf. oraz materiały video) i laboratoriów praktycznych **na platformie OffSec**
- Jedno podejście do egzaminu certyfikacyjnego wliczone w cenę.
- Ponad 50 laboratoriów Proving Grounds Play – symulacje ataków w realistycznym środowisku.

Warunki uczestnictwa

Ten kurs jest przeznaczony dla osób z solidnymi podstawami w zakresie bezpieczeństwa ofensywnego.

Oczekujemy od uczestników ukończenia kursu PEN-200 i zdania egzaminu OSCP+ lub posiadania równoważnej wiedzy i doświadczenia.

Uczestnicy powinni swobodnie posługiwać się systemami operacyjnymi, sieciami TCP/IP, pisać skrypty (np. w Pythonie lub Bash) oraz posiadać podstawową wiedzę o tworzeniu exploitów.

Warunki techniczne

Realizacja za pomocą platformy e-learningowej OffSec https://portal.offsec.com

Wymagania sprzętowe:

- komputer z dostępem do internetu o minimalnej przepustowości 20Mb/s.

- wbudowane lub peryferyjne urządzenia do obsługi audio - słuchawki/głośniki oraz mikrofon.

- zainstalowana przeglądarka internetowa - Microsoft Edge/ Internet Explorer 10+ / **Google Chrome** 39+ (sugerowana) / Safari 7+

Kontakt

Ewa Kasprzak

E-mail ewa.kasprzak@softronic.pl
Telefon (+48) 618 658 840