Możliwość dofinansowania

PEN-201 Testy penetracyjne i ethical hacking w praktyce (Introduction to Ethical Hacking) - szkolenie

Numer usługi 2026/07/30/18395/3719215

2 900,00 PLN brutto
2 900,00 PLN netto
138,10 PLN brutto/h
138,10 PLN netto/h
261,33 PLN cena rynkowa

Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie

4,6 / 5

45 ocen

Usługa szkoleniowa
zdalna w czasie rzeczywistym
Zajęcia grupowe
21:00 h
05.10.2026 do 07.10.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Specjaliści ds. cyberbezpieczeństwa (Blue Team), którzy chcą poznać perspektywę atakującego, administratorzy systemów i sieci planujący transfer do zespołów ofensywnych (Red Team / Pentesting), inżynierowie DevSecOps oraz audytorzy techniczni z firm komercyjnych, instytucji finansowych i administracji publicznej.
Minimalna liczba uczestników	8
Maksymalna liczba uczestników	24
Data zakończenia rekrutacji	01-10-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Podstawa uzyskania wpisu do BUR	art. 163 ust. 1 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (t. j. Dz. U. z 2024 r. poz. 1571, z późn. zm.)
Zakres uprawnień	kształcenie w innych formachkształcenia prowadzonych przez uczelnie

Cel

Cel edukacyjny

Celem szkolenia PEN-201 jest wprowadzenie uczestników w praktyczne podstawy etycznego hackingu oraz metodykę prowadzenia testów penetracyjnych w kontrolowanym środowisku. Uczestnicy poznają pełny cykl testu bezpieczeństwa:

od rekonesansu i skanowania, przez identyfikację oraz eksploatację podatności, aż po eskalację uprawnień, dokumentowanie wyników i przygotowanie rekomendacji naprawczych.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Planuje test penetracyjny zgodnie z zasadami prawnymi i metodykami branżowymi	rozróżnia role cyberprzestępcy, Red Teamu i pentestera, interpretuje zapisy umów RoE/NDA, dobiera metodykę prowadzenia testu adekwatną do zakresu zlecenia	Test teoretyczny
Przeprowadza rekonesans pasywny i aktywny wobec wskazanego celu	zbiera informacje o celu za pomocą narzędzi OSINT bez bezpośredniej interakcji z infrastrukturą, mapuje topologię sieci i identyfikuje aktywne hosty, skanuje porty i usługi technikami Nmap z omijaniem prostych zabezpieczeń	Test teoretyczny
Przeprowadza enumerację usług sieciowych i ocenę podatności	pozyskuje informacje z otwartych usług (bez uwierzytelnienia), wykonuje skan podatności narzędziem automatycznym i klasyfikuje wyniki, odróżnia rzeczywiste podatności od false positives poprzez manualną weryfikację	Test teoretyczny
Przeprowadza kontrolowaną eksploatację podatności i łamie przechwycone hasła	uzyskuje wstępny dostęp do podatnej maszyny przy użyciu Metasploit Framework, rozróżnia typy shelli i payloadów, łamie przechwycone skróty haseł	Test teoretyczny
Przeprowadza eskalację uprawnień oraz opracowuje profesjonalny raport z testu penetracyjnego	identyfikuje wektory eskalacji uprawnień na systemach Linux i Windows i uzyskuje dostęp administracyjny, strukturyzuje raport, formułuje rekomendacje naprawcze uzasadnione kosztowo	Test teoretyczny

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

1. Prawo, etyka i metodyka testów penetracyjnych: RoE, NDA, PTES, OWASP, OSSTMM.
2. Rekonesans pasywny i aktywny: OSINT, Shodan, Censys, WHOIS, mapowanie sieci, skanowanie portów i usług.
3. Enumeracja i identyfikacja podatności: analiza usług sieciowych, skanowanie podatności, CVE/CVSS, weryfikacja false positives.
4. Eksploatacja i ataki na uwierzytelnianie: Metasploit, reverse shell, password cracking, Hashcat, John the Ripper.
5. Post-eksploatacja i eskalacja uprawnień: looting, privilege escalation na systemach Linux i Windows.
6. Raportowanie: przygotowanie executive summary, części technicznej i rekomendacji naprawczych.

Warunki organizacyjne: szkolenie grupowe dla 8–24 uczestników, realizowane na platformie przeznaczonej do pracy zdalnej MS Teams. Uczestnicy pracują na materiałach elektronicznych udostępnionych przez prowadzącego. Walidacja ma formę testu końcowego online prowadzonego przez osobę walidującą odrębną od osoby prowadzącej szkolenie.

Szkolenie realizowane jest zdalnie w czasie rzeczywistym w dniach 5–7.10.2026, z jedną 60-minutową przerwą każdego dnia oraz 30-minutowym testem teoretycznym online kończącym szkolenie w dniu 7.10.2026.

Harmonogram

Liczba pozycji harmonogramu: 13

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 13 Moduł 1: Aspekty prawne, etyka i metodyka testów penetracyjnych	Zajęcia	Paweł Skalny	05-10-2026	08:00	08:45	00:45
2 z 13 Moduł 2: Rekonesans pasywny (OSINT)	Zajęcia	Paweł Skalny	05-10-2026	08:45	10:15	01:30
3 z 13 -	Przerwa	-	05-10-2026	10:15	11:15	01:00
4 z 13 Moduł 3: Rekonesans aktywny	Zajęcia	Paweł Skalny	05-10-2026	11:15	12:45	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 13 Moduł 4: Enumeracja usług sieciowych	Zajęcia	Paweł Skalny	05-10-2026	12:45	15:00	02:15
6 z 13 Moduł 5: Skanowanie podatności	Zajęcia	Paweł Skalny	06-10-2026	08:00	10:15	02:15
7 z 13 -	Przerwa	-	06-10-2026	10:15	11:15	01:00
8 z 13 Moduł 6: Eksploatacja	Zajęcia	Paweł Skalny	06-10-2026	11:15	14:00	02:45
9 z 13 Moduł 7: Ataki na uwierzytelnianie	Zajęcia	Paweł Skalny	07-10-2026	08:00	09:30	01:30
10 z 13 Moduł 8: Post-eksploatacja i eskalacja uprawnień	Zajęcia	Paweł Skalny	07-10-2026	09:30	12:30	03:00
11 z 13 -	Przerwa	-	07-10-2026	12:30	13:30	01:00
12 z 13 Moduł 9: Raportowanie z testu penetracyjnego	Zajęcia	Paweł Skalny	07-10-2026	13:30	15:30	02:00
13 z 13 -	Walidacja	-	07-10-2026	15:30	16:00	00:30

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	21:00
w tym suma godzin zajęć	17:30
w tym suma godzin walidacji	00:30
w tym suma przerw	03:00

Rodzaj godzin	Liczba godzin
Suma godzin dydaktycznych bez przerw	24:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 900,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	2 900,00 PLN
Koszt osobogodziny brutto	138,10 PLN
Koszt osobogodziny netto	138,10 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	21:00

Prowadzący

Liczba prowadzących: 1

1 z 1

Paweł Skalny

Specjalista ds. bezpieczeństwa w AGH, związany zawodowo z obszarem testów penetracyjnych aplikacji webowych oraz serwerów. Posiada praktyczne doświadczenie w pracy z narzędziami i środowiskami wykorzystywanymi w bezpieczeństwie ofensywnym, takimi jak Kali Linux, Burp Suite i Nessus, a także w pracy z systemami Windows oraz językami programowania, m.in. C, C++, Python i Rust.
Posiada certyfikat OSCP Offensive Security. Interesuje się kryptografią, rozwiązywaniem zadań CTF oraz tworzeniem oprogramowania. W szkoleniach łączy podejście praktyczne z naciskiem na etykę, metodykę i rzetelne raportowanie wyników testów bezpieczeństwa.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymają materiały bezpośrednio związane z realizowaną usługą oraz dokument potwierdzający udział/ukończenie szkolenia po zdaniu testu teoretycznego.

Warunki techniczne

1. Sprzęt komputerowy

Uczestnik zobowiązany jest do korzystania z komputera lub laptopa wyposażonego w:

- system operacyjny Windows 10/11, macOS lub Linux,
- procesor klasy **Intel i5 / Ryzen 5** lub równoważny,
- minimum **8 GB RAM** (zalecane 16 GB),
- co najmniej **10 GB wulnej przestrzeni dyskowej**,
- stabilne łącze internetowe o przepustowości **min. 10 Mbps**,
- aktualną przeglądarkę internetową: Chrome, Edge lub Firefox.

2. Wyposażenie audiowizualne

Uczestnik musi posiadać:

- **sprawną kamerę** (wbudowaną lub zewnętrzną), umożliwiającą udział w zajęciach, ćwiczeniach oraz interakcję z prowadzącym,
- **sprawny głośnik i mikrofon** (wbudowany lub zewnętrzny), niezbędny do komunikacji podczas zajęć. Zaleca się korzystanie z **słuchawek z mikrofonem** w celu poprawy jakości dźwięku i redukcji zakłóceń.

3. Środowisko szkoleniowe

Szkolenie realizowane jest z wykorzystaniem platformy umożliwiającej:

- **udostępnianie ekranu** przez prowadzącego i uczestników,
- **komunikację audio-wideo oraz czat** w celu zapewnienia interaktywnego udziału w zajęciach,
- **współdzielenie materiałów i plików** niezbędnych do realizacji programu szkulenia,
- **interaktywną prezentację kodu i analiz danych**, w tym wykonywanie ćwiczeń praktycznych w czasie rzeczywistym.

Kontakt

Agata Rzepka

E-mail szkolenia@informatyka.agh.edu.pl

Telefon (+48) 12 3283 414