



Uniwersytet WSB
Merito w Gdańsku



Pentester – tester cyberbezpieczeństwa

Numer usługi 2025/04/10/7100/2682607

📍 zdalna w czasie rzeczywistym

📖 Studia podyplomowe

🕒 160 h

📅 18.10.2025 do 28.06.2026

8 200,00 PLN brutto

8 200,00 PLN netto

51,25 PLN brutto/h

51,25 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Kierunek skierowany jest do osób posiadających doświadczenie w branży IT: • Junior Testerów i Junior Programistów / Developerów • Absolwentów kierunków informatycznych • Pasjonatów cyberbezpieczeństwa
Minimalna liczba uczestników	20
Maksymalna liczba uczestników	36
Data zakończenia rekrutacji	13-10-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	160
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 2023 r. poz. 742, z późn. zm.)
Zakres uprawnień	Studia podyplomowe

Cel

Cel edukacyjny

Celem studiów jest tworzenie specjalistów o globalnym spojrzeniu na cyberbezpieczeństwo. Dążymy do wykształcenia profesjonalistów zdolnych nie tylko do rozpoznawania zagrożeń, ale przede wszystkim do aktywnego przeciwdziałania atakom cybernetycznym. Naszym celem jest tworzenie bezpiecznej przestrzeni cyfrowej poprzez rozwijanie umiejętności testowania, zabezpieczania i świadomej reakcji na zagrożenia.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
WIEDZA - Tłumaczy zasady bezpieczeństwa w sieci i testy penetracyjne. - Omawia temat bezpieczeństwa systemów operacyjnych - Wyjaśnia zasady przeprowadzania testów penetracyjne aplikacji mobilnych oraz webowych.	 - Objaśnia podstawy testów penetracyjnych, metody analizy incydentów oraz zabezpieczeń sieciowych. - Tłumaczy architekturę systemów operacyjnych, w tym systemu Windows, oraz specyficzne zagrożenia związane z tymi systemami.	Test teoretyczny z wynikiem generowanym automatycznie
		Wywiad ustrukturyzowany Prezentacja
UMIEJĘTNOŚCI - Analizuje incydenty i reaguje na nie. - Zabezpiecza aplikacje webowe i mobilne. - Wykorzystuje narzędzia do testów penetracyjnych	 - Identyfikuje przyczyny oraz sposoby zapobiegania ich wystąpieniu w przyszłości. - Stosuje odpowiednie techniki zabezpieczające aplikacje webowe oraz mobilne przed popularnymi atakami. - Korzysta z takich narzędzi jak Burp Suite, Kali Linux, Metasploit czy OWASP ZAP.	Wywiad ustrukturyzowany
		Prezentacja
KOMPETENCJE SPOŁECZNE - Posiada zdolności analityczne i skutecznie rozwiązuje problemy - Wykorzystuje zasady etyki zawodowej i odpowiedzialności.	 - Rozwija zdolności analityczne, które pozwolą identyfikować zagrożenia i przeprowadzać skuteczne testy penetracyjne. - Rozwija swoją świadomość o etycznych aspektach swojej pracy jako pentesterzy (zachowanie zasad poufności i odpowiedzialności podczas przeprowadzania testów penetracyjnych).	Wywiad ustrukturyzowany
		Prezentacja

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

Efekty uczenia oraz sposoby ich weryfikacji.

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

Tak

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

Tak

Program

Bezpieczeństwo Sieci i testy penetracyjne (27 godz.)

- Wprowadzenie do tematyki testów penetracyjnych
- Bezpieczeństwo sieci
- Testy penetracyjne sieci
- Analiza incydentów

Bezpieczeństwo Systemów Operacyjnych (21 godz.)

- Architektura systemu Windows
- Analiza incydentów typowych dla Windowsa
- Kryptografia w Windows

Bezpieczeństwo aplikacji Mobile (27 godz.)

- Architektura aplikacji mobilnych
- Podstawowe ataki na aplikacje mobilne
- Metody przeciwdziałania

Bezpieczeństwo aplikacji Web (31 godz.)

- Architektura aplikacji webowych
- Podstawowe ataki na aplikacje webowe
- Metody przeciwdziałania

Testy penetracyjne aplikacji Web (27 godz.)

- Cykl testów penetracyjnych aplikacji
- Narzędzia do wykonywania testów penetracyjnych aplikacji www
- Definiowanie wymagań bezpieczeństwa dla aplikacji

Testy penetracyjne aplikacji Mobile (27 godz.)

- Wstęp do anatomii ataków na aplikacje mobilne
- Skanowanie aplikacji
- Mechanizmy zabezpieczeń aplikacji

Harmonogram

Liczba przedmiotów/zajęć: 1

Przedmiot / temat zajęć	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 1 Wprowadzenie do studiów	18-10-2025	08:00	16:00	08:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	8 200,00 PLN
Koszt przypadający na 1 uczestnika netto	8 200,00 PLN
Koszt osobogodziny brutto	51,25 PLN
Koszt osobogodziny netto	51,25 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Rafał Gołębiowski

Menedżer ds. cyberbezpieczeństwa z doświadczeniem w pracy w bankowości, firmach informatycznych oraz konsultingowych. Odpowiedzialny zarówno za ofensywne, jak i defensywne aspekty bezpieczeństwa. W obecnej firmie Hitachi ABB Power Grids, jest szefem globalnego departamentu cyberbezpieczeństwa.

Dodatkowo prowadzi szkolenia z bezpieczeństwa IT. Prowadził szkolenia dla takich organizacji jak Komenda Główna Policji, Centralne Laboratorium Kryminalistyczne Policji, Ministerstwo Rodziny Pracy i Polityki Społecznej, PZU, GUS oraz ZUS.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały elektroniczne zamieszczane na moodlu/temsach.

Dodatkowo wymagany jest zapis przez formularz rekrutacyjny uczelni

<https://www.merito.pl/rekrutacja/krok1>

Warunki uczestnictwa

Szczegółowe informacje na temat rekrutacji znajdują się pod linkiem:

<https://www.merito.pl/gdansk/studia-i-szkolenia/studia-podyplomowe/zasady-rekrutacji>

Warunki techniczne

Wymagania: posiadanie sprzętu elektronicznego z dostępem do internetu, monitor, klawiatura.

Uczelnia zapewnia dostęp do platformy TEAMS.

Kontakt



Agata Orlich

E-mail rekrutacjasp@gdansk.merito.pl

Telefon (+48) 585 227 513