



Uniwersytet WSB
Merito w Poznaniu



Pentester - specjalista ds. cyberbezpieczeństwa

Numer usługi 2025/03/31/7405/2659615

📍 zdalna w czasie rzeczywistym

📖 Studia podyplomowe

🕒 160 h

📅 25.10.2025 do 30.06.2026

8 550,00 PLN brutto

8 550,00 PLN netto

53,44 PLN brutto/h

53,44 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikator projektu	Kierunek - Rozwój
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: <ul style="list-style-type: none">• Junior Testerów i Junir Programistów/Developerów• Absolwentów kierunków informatycznych• Pasjonatów cyberbezpieczeństwa Usługa adresowana również dla Uczestników Projektu Kierunek – Rozwój.
Minimalna liczba uczestników	18
Maksymalna liczba uczestników	25
Data zakończenia rekrutacji	16-10-2025
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 kierunku jest: Wykształcenie specjalistów zdolnych do wykrywania i przeciwdziałania atakom cybernetycznym, w tym przeprowadzania testów penetracyjnych w celu zapewnienia bezpieczeństwa danych i infrastruktury IT.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Opisuje narzędzia oraz technologie związane z bezpieczeństwem sieci oraz systemów operacyjnych	<ul style="list-style-type: none">- przedstawia tematykę bezpieczeństwa sieci- przedstawia tematykę bezpieczeństwa systemów operacyjnych	Test teoretyczny
Definiuje rodzaje testów penetracyjnych	<ul style="list-style-type: none">- opisuje rodzaje testów penetracyjnych- analizuje anatomię ataków na aplikacje webowe oraz mobilne mobilne	Test teoretyczny
Wyjaśnia zasady bezpieczeństwa aplikacji webowych oraz mobilnych	<ul style="list-style-type: none">- opisuje architekturę aplikacji webowych oraz mobilnych- przedstawia metody przeciwdziałania atakom na aplikacje webowe oraz mobilne	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

Świadectwo studiów podyplomowych zawiera program kierunku wraz ze zrealizowanymi godzinami i punktami ECTS. Absolwent uzyskuje zaświadczenie potwierdzające zdobyte efekty kształcenia.

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

Świadectwo ukończenia studiów podyplomowych jest wydawane na podstawie uzyskania pozytywnej oceny z każdego semestru zgodnie z Regulaminem Studiów Podyplomowych.

Studia kończą się zaliczeniem na ocenę określonym w karcie kierunku.

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

Świadectwo ukończenia studiów podyplomowych jest potwierdzeniem uzyskania pozytywnego wyniku z testu semestralnego i egzaminu końcowego.

Program

Nazwa modułu/obszaru z programu studiów (wraz z liczbą godzin)	Wylistowane poszczególne przedmioty, w ramach tego modułu/obszaru (wraz z liczbą godzin)
1. Bezpieczeństwo Sieci i testy penetracyjne (27 godz.)	<ul style="list-style-type: none">• Wprowadzenie do tematyki testów penetracyjnych• Bezpieczeństwo sieci• Testy penetracyjne sieci• Analiza incydentów
2. Bezpieczeństwo Systemów Operacyjnych (21 godz.)	<ul style="list-style-type: none">• Architektura systemu Windows• Analiza incydentów typowych dla Windowsa• Kryptografia w Windows
3. Bezpieczeństwo aplikacji Mobile (27 godz.)	<ul style="list-style-type: none">• Architektura aplikacji mobilnych• Podstawowe ataki na aplikacje mobilne• Metody przeciwdziałania
4. Bezpieczeństwo aplikacji Web (31 godz.)	<ul style="list-style-type: none">• Architektura aplikacji webowych• Podstawowe ataki na aplikacje webowe• Metody przeciwdziałania
5. Testy penetracyjne aplikacji Web (27 godz.)	<ul style="list-style-type: none">• Cykl testów penetracyjnych aplikacji• Narzędzia do wykonywania testów penetracyjnych aplikacji www• Definiowanie wymagań bezpieczeństwa dla aplikacji
6. Testy penetracyjne aplikacji Mobile (27 godz.)	<ul style="list-style-type: none">• Wstęp do anatomii ataków na aplikacje mobilne• Skanowanie aplikacji• Mechanizmy zabezpieczeń aplikacji

Łączna ilość godzin 160 (jedna godzina lekcyjna = 45 minut)

Harmonogram

Liczba przedmiotów/zajęć: 0

Przedmiot / temat zajęć	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
-------------------------	-----------------------	---------------------	---------------------	---------------

Brak wyników.

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	8 550,00 PLN

Koszt przypadający na 1 uczestnika netto	8 550,00 PLN
Koszt osobogodziny brutto	53,44 PLN
Koszt osobogodziny netto	53,44 PLN

Prowadzący

Liczba prowadzących: 3



1 z 3

Anita Łukowska

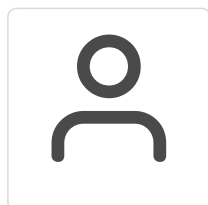
Absolwentka Politechniki Poznańskiej na kierunku Informatyka. Pentesterka, programistka, uczestniczka zawodów Capture The Flag. Zawodowo zajmuje się zagadnieniami związanymi z bezpieczeństwem aplikacji webowych oraz procesem tworzenia bezpiecznego oprogramowania. Posiada doświadczenie w zakresie DevSecOps oraz zarządzania bezpieczeństwem baz danych i systemów operacyjnych. Prywatnie wieloletnia wolontariuszka w fundacji opiekującej się zwierzętami.



2 z 3

Michał Kucharski

Absolwent Politechniki Śląskiej na kierunku Informatyka Przemysłowa, więc oprócz dyskusji z komputerem rozumie układ żelazo-węgiel (mniej więcej). Aktywny administrator portalu internetowego, zarówno od strony technicznej jak i programistycznej, co w dzisiejszych czasach czyni go DevOpsem. Człowiek, który szybko pochłania nowe technologie i wzorce projektowe, mimo iż dalej jest fanem Windowsa XP. Chętnie dzieli się zdobytą wiedzą udzielając się w wielu społecznościach IT Sec / Developing / Programming. Uczestnik wielu imprez typu Hackaton i Capture The Flag, gracz HackTheBox. Zawodowo szlifuje swoje umiejętności w zespole łączącym defensywne i ofensywne podejście do bezpieczeństwa IT – purple team.



3 z 3

Kacper Nizioł

Przeprowadziłem liczne udane testy penetracyjne dla różnorodnych klientów, identyfikując i raportując podatności oraz dostarczając konkretnych zaleceń w celu poprawy ich poziomu bezpieczeństwa. Aktywnie udzielam się na platformie HackTheBox, która pozwala mi na ciągły rozwój umiejętności poprzez rozwiązywanie zadań, udział w rywalizacji oraz dzielenie się wiedzą z innymi członkami zespołu AlphaPwners. Posiadam głęboką wiedzę na temat różnorodnych typów ataków, technik wykorzystywanych przez cyberprzestępców oraz sposobów obrony przed nimi. Dodatkowo, moje doświadczenie w pracy zespołowej jest niezwykle wartościowe. Pracując nad projektami zespołowymi, zawsze stawiam na skuteczną komunikację, wymianę pomysłów oraz współpracę w celu osiągnięcia wspólnego celu. W mojej przyszłej karierze chciałbym skupić się na rozwoju w dziedzinach, takich jak testowanie aplikacji mobilnych czy głębsze poznanie metod testów Active Directory. Obecnie przygotowuję się do certyfikatu OSCP.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Podczas zjazdu każdy uczestnik programu otrzymuje komplet materiałów dydaktycznych w formie pdf bądź na platformie moodle. Materiały te przygotowują wykładowcy, dostosowując je do specyfiki prowadzonego tematu.

Uczestnicy studiów pracują na platformie Extranet, to wewnętrzna platforma komunikacyjna Uczelni WSB Merito, stworzona w celu ograniczenia formalności oraz ułatwienia przepływu informacji między uczestnikami a uczelnią. Za jej pomocą przez całą dobę i z każdego miejsca na świecie uczestnicy mają dostęp do:

- harmonogramu zajęć,
- informacji na temat płatności,
- materiałów dydaktycznych,
- katalogu bibliotecznego,
- informacji dotyczących zmian w planach zajęć, ogłoszeń i aktualności.

Warunki uczestnictwa

Zapisu można dokonać na stronach Uniwersytetu WSB Merito w wybranych filiach w:

- Chorzowie,
- Poznaniu,
- Szczecinie,
- Warszawie

poprzez formularz online znajdujący się na stronie: www.wsb.pl/rekrutacja/krok1 oraz dostarczyć komplet dokumentów do Biura Rekrutacji do wybranej filii.

Kryteria uczestnictwa w Programie

- ukończone studia wyższe I lub II stopnia
- spełnienie warunków rekrutacyjnych

Warunki zaliczenia

test końcowy

Interaktywna forma zajęć

Wykłady uzupełniane są ćwiczeniami, warsztatami, studiami przypadków, treningami i symulacją biznesową, dzięki którym uczestnicy mogą na bieżąco weryfikować swoje umiejętności.

Zjazdy odbywają się średnio raz lub dwa razy w miesiącu:

- w soboty i niedziele w godzinach 8:00 - 15:00

Informacje dodatkowe

- Szczegółowy harmonogram usługi może ulec zmianie w postaci realizowanych przedmiotów w danym dniu i osób prowadzących.
- Godziny zajęć podane w harmonogramie są godzinami zegarowymi, zaś ilość godzin programowych jest podana w godzinach dydaktycznych. 8 godzin dydaktycznych = 6 godzin zegarowych (160h dydaktycznych = 120h zegarowych)
- Cena usługi nie obejmuje opłaty wpisowej oraz końcowej.
- Cena usługi ulega zmianie, przy rozłożeniu płatności na raty.
- **Zawarto umowę z WUP w Toruniu w ramach Projektu Kierunek - Rozwój.**

Warunki techniczne

Zajęcia odbywają się na platformie MS Teams. Każdy z uczestników zobowiązany jest do posiadania własnego sprzętu z aktywnym mikrofonem, kamerą i dostępem do internetu.

Kontakt



Dział Studiów Podyplomowych

E-mail dsp@warszawa.merito.pl

Telefon (+48) 22 2562 317