



## Specjalista ds. cyberbezpieczeństwa - pentester (studia online).

Numer usługi 2024/10/09/165297/2352522

7 800,00 PLN brutto

7 800,00 PLN netto

48,75 PLN brutto/h

48,75 PLN netto/h

Uniwersytet WSB  
Merito w Toruniu  
Wydział Finansów i  
Zarządzania w  
Bydgoszczy

Brak ocen dla tego dostawcy

📍 zdalna w czasie rzeczywistym

📚 Studia podyplomowe

🕒 160 h

📅 26.10.2024 do 30.06.2025

## Informacje podstawowe

<b>Kategoria</b>	Informatyka i telekomunikacja / Bezpieczeństwo IT
<b>Sposób dofinansowania</b>	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
<b>Grupa docelowa usługi</b>	Studia kierowane są do: <ul style="list-style-type: none"><li>dla absolwentów kierunków informatycznych,</li><li>dla Junior Testerów i Junior Programistów/Developerów,</li><li>dla pasjonatów cyberbezpieczeństwa.</li></ul> Usługa jest adresowana również do uczestników projektu KIERUNEK - ROZWÓJ, podpisano umowę ramową z WUP TORUŃ celem rozliczania bonów.
<b>Minimalna liczba uczestników</b>	15
<b>Maksymalna liczba uczestników</b>	30
<b>Data zakończenia rekrutacji</b>	21-10-2024
<b>Forma prowadzenia usługi</b>	zdalna w czasie rzeczywistym
<b>Liczba godzin usługi</b>	160
<b>Podstawa uzyskania wpisu do BUR</b>	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.)
<b>Zakres uprawnień</b>	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
wiedza: Zdobędziesz wiedzę dotyczącą sposobów zabezpieczania produktów i usług IT.	test wiedzy zabezpieczania produktów i usług IT	Test teoretyczny
umiejętności: umiesz przeprowadzać testy penetracyjne aplikacji i systemów wcielając się w rolę potencjalnego hackera.	case study	Analiza dowodów i deklaracji

# 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 końcowej 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 egzaminu końcowego.

# Program

(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

#### FORMA ZALICZENIA

Test końcowy- walidacja usługi na ostatnim zjeździe

## Harmonogram

Liczba przedmiotów/zajęć: 29

Przedmiot / temat zajęć	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 29 Bezpieczeństwo sieci i testy penetracyjne	26-10-2024	08:00	09:15	01:15
2 z 29 Bezpieczeństwo sieci i testy penetracyjne	26-10-2024	09:45	11:15	01:30
3 z 29 Bezpieczeństwo sieci i testy penetracyjne	26-10-2024	11:30	13:00	01:30
4 z 29 Bezpieczeństwo sieci i testy penetracyjne	26-10-2024	13:30	15:00	01:30
5 z 29 Bezpieczeństwo sieci i testy penetracyjne	09-11-2024	08:00	09:30	01:30
6 z 29 Specjalista ds. cyberbezpieczeństwa - pentester	09-11-2024	09:45	11:15	01:30
7 z 29 Bezpieczeństwo sieci i testy penetracyjne	09-11-2024	11:30	13:00	01:30
8 z 29 Bezpieczeństwo sieci i testy penetracyjne	09-11-2024	13:30	15:00	01:30
9 z 29 Bezpieczeństwo sieci i testy penetracyjne	09-11-2024	15:15	16:45	01:30
10 z 29 Bezpieczeństwo sieci i testy penetracyjne	10-11-2024	08:00	09:30	01:30
11 z 29 Bezpieczeństwo sieci i testy penetracyjne	10-11-2024	09:45	10:30	00:45
12 z 29 Bezpieczeństwo aplikacji web	10-11-2024	11:30	13:00	01:30
13 z 29 Bezpieczeństwo aplikacji web	10-11-2024	13:30	15:00	01:30

Przedmiot / temat zajęć	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
14 z 29 Specjalista ds. cyberbezpieczeństwa - pentester	30-11-2024	08:00	16:00	08:00
15 z 29 Specjalista ds. cyberbezpieczeństwa - pentester	01-12-2024	08:00	16:00	08:00
16 z 29 Specjalista ds. cyberbezpieczeństwa - pentester	07-12-2024	08:00	16:00	08:00
17 z 29 Specjalista ds. cyberbezpieczeństwa - pentester	08-12-2024	08:00	16:00	08:00
18 z 29 Specjalista ds. cyberbezpieczeństwa - pentester	11-01-2025	08:00	16:00	08:00
19 z 29 Specjalista ds. cyberbezpieczeństwa - pentester	12-01-2025	08:00	16:00	08:00
20 z 29 Specjalista ds. cyberbezpieczeństwa - pentester	08-02-2025	08:00	16:00	08:00
21 z 29 Specjalista ds. cyberbezpieczeństwa - pentester	09-02-2025	08:00	16:00	08:00
22 z 29 Specjalista ds. cyberbezpieczeństwa - pentester	15-02-2025	08:00	16:00	08:00
23 z 29 Specjalista ds. cyberbezpieczeństwa - pentester	16-02-2025	08:00	16:00	08:00
24 z 29 Specjalista ds. cyberbezpieczeństwa - pentester	01-03-2025	08:00	16:00	08:00
25 z 29 Specjalista ds. cyberbezpieczeństwa - pentester	02-03-2025	08:00	16:00	08:00
26 z 29 Specjalista ds. cyberbezpieczeństwa - pentester	12-04-2025	08:00	16:00	08:00

Przedmiot / temat zajęć	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>27 z 29</b> Specjalista ds. cyberbezpieczeństwa - pentester	13-04-2025	08:00	16:00	08:00
<b>28 z 29</b> Specjalista ds. cyberbezpieczeństwa - pentester	17-05-2025	08:00	16:00	08:00
<b>29 z 29</b> Specjalista ds. cyberbezpieczeństwa - pentester/ walidacja usługi	18-05-2025	08:00	16:00	08:00

## Cennik

### Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	7 800,00 PLN
Koszt przypadający na 1 uczestnika netto	7 800,00 PLN
Koszt osobogodziny brutto	48,75 PLN
Koszt osobogodziny netto	48,75 PLN

## Prowadzący

Liczba prowadzących: 3



**1 z 3**

### Michał Kucharski

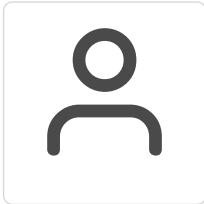
Absolwent Politechniki Śląskiej na kierunku Informatyka Przemysłowa, więc oprócz dyskusji z komputerem rozumie układ żelazo-węgiel (mniej więcej). Aktywny administrator portalu internetowego, zarówno od strony technicznej jak i programistycznej, co w dzisiejszych czasach czyni go DevOpsem. Człowiek, 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. Wielbiciel sportów ekstremalnych takich jak układanie kostek Rubika oraz montaż układów z pochodnych Arduino. Kiedyś powiedziałem "Wiem, że jeszcze wiele nie wiem, ale się dowiem" i wciąż się tego trzymam.



2 z 3

## Kacper Nizioł

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



3 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.

# Informacje dodatkowe

## Informacje o materiałach dla uczestników usługi

Uczestnicy studiów podyplomowych otrzymują dodatkowe materiały na zajęciach oraz po, które są zamieszczane na platformie MS Teams.

Podczas zjazdu każdy uczestnik programu otrzymuje komplet materiałów dydaktycznych na platformie MS Teams. Materiały te przygotowują wykładowcy, dostosowując je do specyfiki prowadzonego tematu.

Uczestnicy studiów pracują na platformie MS Teams, to 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,
- materiałów dydaktycznych,
- informacji dotyczących zmian w planach zajęć, ogłoszeń i aktualności.

## Warunki uczestnictwa

Uczestnikiem studiów podyplomowych na Uniwersytecie WSB Merito w Toruniu filia w Bydgoszczy, może zostać każda osoba w wykształceniu wyższym (licencjackim, inżynierskim lub magisterskim). O przyjęciu na studia decyduje kolejność zgłoszeń.

## Informacje dodatkowe

### Informacje dodatkowe

- Szczegółowy harmonogram usługi może ulec zmianie w postaci realizowanych przedmiotów w danym dniu i osób prowadzących. **Zmianie nie ulegają godziny usługi.**
- **Harmonogram zjazdów zostanie upubliczniony na stronach Uczelni**

- Godziny zajęć podane w harmonogramie są godzinami zegarowymi, zaś ilość godzin programowych jest podana w godzinach dydaktycznych.

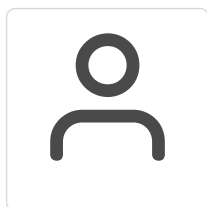
Usługa dostępna również dla uczestników projektu KIERUNEK ROZWÓJ- podpisano umowę ramową z WUP TORUŃ celem rozliczania bonów

## Warunki techniczne

Techniczne wymagania do zajęć:

- komputer (z wbudowanymi lub podłączonymi głośnikami i mikrofonem),
- dostęp do Internetu,
- słuchawki (opcjonalnie),
- jeśli chcesz aby Cię widziano, możesz użyć kamery umieszczonej w laptopie/komputerze.

## Kontakt



**Katarzyna Lis**

**E-mail** [katarzyna.lis@torun.merito.pl](mailto:katarzyna.lis@torun.merito.pl)

**Telefon** (+48) 787 638 120