KARTA PRZEDMIOTU

Kod przedmiotu	studia stacjonarne:	E-ID2C-15-s2, E-ID2C-15-s3
	studia niestacjonarne:	E-2IZ2C-1019-s3
Nazwa przedmiotu	**Testy penetracyjne**	
Nazwa przedmiotu w języku angielskim	**Penetration Tests**	
Obowiązuje od roku akademickiego	**2023/24**	

USYTUOWANIE PRZEDMIOTU W SYSTEMIE STUDIÓW

Kierunek studiów	**Informatyka**
Poziom kształcenia	**II stopień**
Profil studiów	**Ogólnoakademicki**
Forma i tryb prowadzenia studiów	**Studia stacjonarne i niestacjonarne**
Zakres	**Cyberbezpieczeństwo**
Jednostka prowadząca przedmiot	**Katedra Systemów Informatycznych**
Koordynator przedmiotu	**dr inż. Arkadiusz Chrobot**
Zatwierdził	**Dziekan Wydziału Elektrotechniki, Automatyki i Informatyki dr hab. inż. Roman Deniziak, prof. PŚk**

OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

Przynależność do grupy/bloku przedmiotów		**Przedmiot specjalnościowy**
Status przedmiotu		**Wybieralny**
Język prowadzenia zajęć		**Polski**
Usytuowanie w planie studiów - semestr	studia stacjonarne	**Semestr II lub Semestr III**
	studia niestacjonarne	**Semestr II lub Semestr III**
Wymagania wstępne		**Audyty bezpieczeństwa**
Egzamin (TAK/NIE)		**NIE**
Liczba punktów ECTS		**3**

Forma prowadzenia zajęć		**wykład**	**ćwiczenia**	**laboratorium**	**projekt**	**inne**
Liczba godzin w semestrze	studia stacjonarne:	**30**			**30**	
	studia niestacjonarne:	**18**			**18**	

EFEKTY UCZENIA SIĘ

Kategoria	Symbol efektu	Efekty uczenia się	Odniesienie do efektów kierunkowych
Wiedza	W01	Zna i rozumie pojęcia przestrzeni ataku i wektora ataku.	INF2_W02
	W02	Zna i rozumie rodzaje podatności oraz techniki ich wykrywania.	INF2_W03
	W03	Zna i rozumie zasady działania narzędzi do testów penetracyjnych.	INF2_W02, INF2_W03
	W04	Zna i rozumie zasady tworzenia raportów z testów penetracyjnych.	INF2_W03
Umiejętności	U01	Potrafi przeprowadzić testy penetracyjne systemów informatycznych.	INF2_U01, INF2_U02, INF2_U05, INF2_U06
	U02	Umie opracować raport z testów penetracyjnych.	INF2_U03, INF2_U06
Kompetencje społeczne	K01	Jest gotów ciągle podnosić swoje kwalifikacje w zakresie testowania penetracyjnego systemów informatycznych.	INF2_K03
	K02	Jest gotów prowadzić testy penetracyjne systemów informatycznych z poszanowanie norm prawnych i etycznych.	INF2_K04

TREŚCI PROGRAMOWE

Forma zajęć	Treści programowe
wykład	1. **Zagrożenia dla bezpieczeństwa systemów informatycznych** (przestrzeń ataku, wektor ataku, model zagrożeń dla aplikacji). 2. **Metodologia testów penetracyjnych** (zalecenia OWASP i inne wytyczne). 3. **Narzędzia do testów penetracyjnych** (zasada działania, struktura, wykorzystanie). 4. **Raportowanie wyników testów penetracyjnych** (ocena zagrożenia – metryka CVSS i inne, opis zidentyfikowanych podatności)
projekt	1. **Planowanie i przygotowanie testów** (określanie przestrzeni i wektorów ataków, uzyskiwanie i systematyzowanie informacji o testowanym systemie) 2. **Przeprowadzanie testów** (wybór i konfiguracja narzędzi, testy manualne, półautomatyczne i automatyczne). 3. **Raportowanie odkrytych podatności** (wyliczanie metryki CVSS, określanie warunków wystąpienia, opis przeprowadzenia ataku i jego skutków, zalecenia).

METODY WERYFIKACJI EFEKTÓW UCZENIA SIĘ

Symbol efektu	Metody sprawdzania efektów uczenia się					
	Egzamin ustny	Egzamin pisemny	Kolokwium	Projekt	Sprawozdanie	Inne
W01			X	X		X
W02			X	X		X
W03			X	X		X
W04			X	X		X
U01				X		X
U02				X		X
K01				X		X

FORMA I WARUNKI ZALICZENIA

Forma zajęć	Forma zaliczenia	Warunki zaliczenia
wykład	zaliczenie z oceną	Na podstawie wyników z projektu lub uzyskanie co najmniej 50% punktów z kolokwium.
projekt	zaliczenie z oceną	Uzyskanie co najmniej 50% punktów za realizację zadania projektowego.

NAKŁAD PRACY STUDENTA

Bilans punktów ECTS												
Lp.	Rodzaj aktywności	Obciążenie studenta										Jednostka
		studia stacjonarne					studia niestacjonarne					
1.	Udział w zajęciach zgodnie z planem studiów	W	C	L	P	S	W	C	L	P	S	h
		30			**30**		**18**			**18**		
2.	Inne (konsultacje, egzamin)	**2**			**2**		**2**			**2**		h
3.	**Razem przy bezpośrednim udziale nauczyciela akademickiego**	**64**					**40**					h
4.	**Liczba punktów ECTS, którą student uzyskuje przy bezpośrednim udziale nauczyciela akademickiego**	**2,56**					**1,6**					ECTS
5.	**Liczba godzin samodzielnej pracy studenta**	**11**					**35**					h
6.	**Liczba punktów ECTS, którą student uzyskuje w ramach samodzielnej pracy**	**0,44**					**1,4**					ECTS
7.	**Nakład pracy związany z zajęciami o charakterze praktycznym**	**30**					**18**					h
8.	**Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym**	**1,20**					**0,72**					ECTS
9.	**Sumaryczne obciążenie pracą studenta**	**75**					**75**					h
10.	**Punkty ECTS za moduł** *1 punkt ECTS=25 godzin obciążenia studenta*	**3**										ECTS

LITERATURA

1. Michał Bentkowski i inni, „Bezpieczeństwo aplikacji webowych”, Securitum Szkolenia, Kraków, 2019
2. Bernhard Mueller, Sven Schleier, Jeroen Willemsen, Carlos Holguera i inni, „MASTG – Mobile Application Security Testing Guide”, OWASP, https://owasp.org/www-project-mobile-app-security/ (dostęp: 15-09-2022)