

KARTA PRZEDMIOTU

Nazwa w języku polskim: **Testy penetracyjne**

Nazwa w języku angielskim: **Penetration testing**

Karta przedmiotu ważna od roku akademickiego: **2022/2023**

Kierunek studiów: **Informatyka**

Poziom studiów: **Studia I stopnia**

Forma studiów: **Niestacjonarne**

Profil: **Praktyczny**

Specjalność: **Cyberbezpieczeństwo**

Język wykładowy: **Polski**

Jednostka prowadząca: **Wydział Nauk Społecznych i Technicznych**

Prowadzący: **dr Grzegorz Jastrzębski**

OBCIĄŻENIE STUDENTA

	Wykład	Konwersatorium	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć dydaktycznych organizowanych przez Uczelnię			20		
Liczba godzin całkowitego nakładu pracy studenta			50		
Forma zaliczenia			Zaliczenie z oceną		
Liczba punktów ECTS			2		

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

Wiedza dotycząca sieci komputerowych – model OSI, struktura pakietów w sieci Ethernet, zasady routingu.

Podstawowa wiedza nt. typowych aplikacji komputerowych.

Znajomość podstaw działania systemów operacyjnych.

CELE PRZEDMIOTU

C1	Znajomość technik stosowanych przy znajdowaniu luk i podatności w systemach informatycznych.
C2	Umiejętność stosowania odpowiednich narzędzi, odnajdujących aktualne zagrożenia dotyczące danego systemu informatycznego.

PRZEDMIOTOWE EFEKTY UCZENIA – PEU	
Z zakresu wiedzy:	
PEU_W01	Zna techniki stosowane przy wykonywaniu testów penetracyjnych.
Z zakresu umiejętności:	
PEU_U01	Potrafi zaplanować działania mające wyszukać luki i podatności.
PEU_U02	Potrafi korzystać z narzędzi informatycznych umożliwiających wykrycie luk i podatności.
PEU_U03	Potrafi rozpoznać aktualne zagrożenia adekwatne dla danego systemu informatycznego.
Z zakresu kompetencji społecznych:	
PEU_K01	Jest świadom odpowiedzialności związanej z wykonywanymi działaniami i gotów jest ją ponosić.

TREŚCI PROGRAMOWE		
Forma zajęć – laboratorium		Liczba godzin
L1	Wprowadzenie, omówienie zasad zalecenia przedmiotu. Metodologia i frameworki.	3
L2	Zbieranie informacji.	3
L3	Wykrywanie luk w zabezpieczeniach.	2
L4	Wykorzystanie luk w zabezpieczeniach.	2
L5	Ataki w systemie lokalnym.	2
L6	Eskalacja uprawnień.	2
L7	Ataki na sieci.	2
L8	Ataki na systemy pomocnicze.	2
L9	Ataki na aplikacje sieciowe. Podsumowanie, zaliczenie.	2
Razem		20

STOSOWANE NARZĘDZIA DYDAKTYCZNE	
1.	Prezentacja treści z wykorzystaniem multimediiów.
2.	Ćwiczenia wykonywane w laboratorium.
3.	Praca własna – studiowanie aktualnej literatury przedmiotu, źródeł internetowych.

METODY I FORMY OCENY
OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA

Formy oceny (F lub P)*	Numer efektu uczenia (przedmiotowego)	Metody oceny osiągnięcia efektu uczenia
F I	PEU_W01, PEU_U01, PEU_U02, PEU_U03, PEU_K01	Ocena za aktywną realizację ćwiczeń laboratoryjnych.
P I	PEU_W01, PEU_U01, PEU_U02, PEU_U03, PEU_K01	Ocena wykonania zadań na zajęciach zaliczeniowych.

*F – ocena formująca (w trakcie semestru), P – ocena podsumowująca (na koniec semestru)

KRYTERIA OCENY
OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA

Nr PEU	Ocena dostateczna	Ocena dobra	Ocena bardzo dobra
PEU_W01	Zna podstawowe techniki związane z wykonywaniem testów penetracyjnych.	Zna różne techniki związane z wykonywaniem testów penetracyjnych.	Zna techniki związane z wykonywaniem testów penetracyjnych, zna ich specyfikę.
PEU_U01	Potrafi wykonać zadane ćwiczenia dotyczące wyszukiwania podatności.	Potrafi wykonać ćwiczenia dotyczące wyszukiwania podatności, szukając narzędzie.	Potrafi wybrać odpowiednie narzędzie w zbiorze dostępnych, do wyszukiwania podatności, najlepiej dobrane do specyfiki badanego systemu.
PEU_U02	Przeprowadza testy z wykorzystaniem wskazanej dokumentacji.	Samodzielnie przeprowadza testy, wykazując się znajomością funkcjonalności stosowanych narzędzi.	Sprawnie i skutecznie przeprowadza testy, wykazując się znajomością funkcjonalności stosowanych narzędzi i ich specyfikę.
PEU_U03	Potrafi wskazać źródła informacji aktualnej wiedzy nt. podatności wskazanego systemu.	Potrafi zweryfikować używane narzędzia używane do wyszukiwania podatności pod kątem aktualności.	Potrafi zweryfikować i uaktualnić używane narzędzia używane do wyszukiwania podatności pod kątem aktualności.
PEU_K01	Dostrzega ogólnie niebezpieczeństwa związane z przeprowadzaniem testów.	Jest gotów wskazać potencjalne niebezpieczeństwa związane z przeprowadzaniem badaniem.	Jest gotów zaplanować badanie, by minimalizować ryzyko związane z jego przeprowadzeniem.

LITERATURA PODSTAWOWA

P. Engebretson, Hacking i testy penetracyjne. Podstawy, Helion 2013.

LITERATURA UZUPEŁNIAJĄCA

G. Khawaja, Kali Linux i testy penetracyjne Biblia, Helion 2022.

V. Jean-Georges, Hardware i testy penetracyjne. Przewodnik po metodach ataku i obrony, Helion 2022.

ŹRÓDŁA INTERNETOWE

<https://nct.nist.gov/repository> - Repozytorium National Institute of Standards and Technology.

<https://attack.mitre.org/> - Wykaz rozpoznanych technik ataku cybernetycznego.

MACIERZ POWIĄZANIA EFEKTÓW UCZENIA DLA PRZEDMIOTU TESTY PENETRACYJNE Z EFEKTAMI UCZENIA NA KIERUNKU INFORMATYKA

Przedmiotowy efekt uczenia	Odniesienie przedmiotowego efektu do efektów uczenia zdefiniowanych dla kierunku studiów i specjalności	Cele przedmiotu	Treści programowe	Numer narzędzia dydaktycznego
PEU_W01	K_W02, K_W03	C1	L1, L3, L4, L7, L8, L9	1
PEU_U01	K_W05	C1, C2	L1, L2, L3, L4	1, 3
PEU_U02	K_U02, K_U06	C1, C2	L3, L5, L7-9	1, 2, 3
PEU_U03	K_U01, K_U04, K_U07	C1, C2	L3, L7-9	1, 3
PEU_K01	K_K02, K_K03, K_K04	C2	L2, L5, L6	1, 2