

KARTA PRZEDMIOTU

Politechnika Białostocka								Wydział Informatyki			
Kierunek studiów		Informatyka						Poziom i forma studiów		pierwszego stopnia stacjonarne	
Grupa przedmiotów / specjalność		Cyberbezpieczeństwo						Profil kształcenia		ogólnoakademicki	
Nazwa przedmiotu		Testy penetracyjne						Kod przedmiotu		INF1TPE	
								Rodzaj zajęć		obieralny	
Formy zajęć i liczba godzin		W	Ć	L	P	Ps	T	S	Semestr	5,6	
		26				30			Punkty ECTS	5	
Program obowiązuje od								2023/2024			
Przedmioty wprowadzające		Sieci komputerowe (INF1SKO), Systemy operacyjne (INF1SOP), Wprowadzenie do systemu Linux (INF1WSL),									
Cele przedmiotu		Przekazanie wiedzy i umiejętności z zakresu metodologii testów penetracyjnych oraz narzędzi stosowanych w audytach bezpieczeństwa. Rozwój praktycznych kompetencji w identyfikacji, analizie i dokumentowaniu podatności w systemach informatycznych. Kształtowanie świadomości etycznej i prawnej w kontekście testów bezpieczeństwa.									
		Odniesienia do frameworka edukacyjnego mikrokompetencji SFIA:									
		Penetration Testing (PENT) - poziom 3									
		Vulnerability Assessment (VUAS) - poziom 3									
		Information Security (SCTY) - poziom 2									
Ramowe treści programowe		Risk Assessment (RIAS) - poziom 2									
		Technical Specialism (TECH) - poziom 3									
		Przedmiot oferuje kompleksowe wprowadzenie do metodologii testów penetracyjnych jako kluczowego elementu współczesnych strategii cyberbezpieczeństwa. Program obejmuje zarówno teoretyczne podstawy jak i praktyczne aspekty przeprowadzania kontrolowanych ataków na systemy informatyczne w celu identyfikacji podatności przed ich wykorzystaniem przez rzeczywistych napastników.									
		Studenci poznają metodyki testów penetracyjnych (PTES, OWASP, OSSTMM), techniki rozpoznania, skanowania, eksploatacji podatności oraz dokumentowania wyników. Szczególny nacisk położony jest na etyczne aspekty testów bezpieczeństwa oraz legalne ramy prowadzenia audytów. Przedmiot rozwija umiejętności w zakresie testowania bezpieczeństwa aplikacji webowych, sieci, systemów operacyjnych i urządzeń mobilnych, a także przygotowuje do tworzenia profesjonalnych raportów z testów penetracyjnych i rekomendacji dotyczących usuwania zidentyfikowanych podatności.									
Inne informacje o przedmiocie								przedmiot kształtuje umiejętności praktyczne			
Wyliczenie:		Nakład pracy studenta związany z:						Godzin ogółem	W tym kontaktowych	W tym praktycznych	
		udziałem w wykładach						26	26		
		udziałem w innych formach zajęć						30	30	30	
		indywidualnym wsparciem merytorycznym procesu uczenia się, udziałem w zaliczeniach organizowanych poza planem zajęć						4	4		
		przygotowaniem do zaliczenia wykładu						15			
		realizacją zadań praktycznych						50		50	
		Razem godzin:						125	60	80	
		Razem punktów ECTS:						5	2.4	3.2	
Zakładane kierunkowe efekty uczenia się								Wiedza	Umiejętności	Kompetencje społeczne	
								INF1_W03	INF1_U07		
								INF1_W08	INF1_U12		
								INF1_W12	INF1_U13		
								INF1_W14	INF1_U14		
									INF1_U17		
Cele i treści ramowe sformułował(a)		dr inż. Andrzej Chmielewski						Data:		12/06/2025	
Realizacja w roku akademickim								2025/2026			
Treści programowe		Wykład									
		1. Wprowadzenie do testów penetracyjnych - definicje, cele, rodzaje (black/white/gray box)									
		2. Metodyki (OSSTMM, PTES, OWASP), ramy prawne i zagadnienia etyczne									
		3. Rekonesans pasywny i aktywny - techniki zbierania informacji (OSINT), footprinting, analiza domen, skanowanie portów, identyfikacja usług									
		4. Skanowanie podatności - narzędzia automatyczne, interpretacja wyników, fałszywie pozytywne wyniki, priorytetyzacja podatności									
		5. Modelowanie zagrożeń - identyfikacja potencjalnych wektorów ataku, budowanie ścieżek ataku (attack paths), analiza ryzyka									
		6. Testy penetracyjne aplikacji webowych - metodyki OWASP, najczęstsze podatności (XSS, CSRF, SQL Injection, broken authentication), narzędzia									
		7. Testy penetracyjne infrastruktury - ataki na sieci, systemy operacyjne, podnoszenie uprawnień, pivoting, przemieszczanie się w sieci									
		8. Bezpieczeństwo mobilne - specyfika testów penetracyjnych aplikacji mobilnych, reverse engineering, analiza statyczna i dynamiczna									
		9. Inżynieria społeczna i ataki socjotechniczne - techniki manipulacji, phishing, pretexting, bezpieczeństwo personelu									
		10.									

Eksploracja podatności - wykorzystywanie zidentyfikowanych słabości, Metasploit Framework, budowanie PoC (Proof of Concept)	
11.	Post-exploitation - działania po uzyskaniu dostępu, utrzymanie dostępu, zacieranie śladów, analiza forensic
12.	Dokumentacja i raportowanie - struktura profesjonalnego raportu, klasyfikacja podatności, formułowanie rekomendacji, Remediation i zarządzanie podatnościami - strategię naprawy, weryfikacja poprawek, zarządzanie cyklem życia podatności
13.	Zaliczenie wykładu
Pracownia specjalistyczna	
1.	Konfiguracja środowiska laboratoryjnego - wirtualne maszyny, narzędzia testów penetracyjnych, platformy ćwiczeniowe (np. OWASP WebGoat, DVWA)
2.	Warsztaty z narzędzi rozpoznania - praktyczne wykorzystanie Nmap, Shodan, theHarvester, Maltego do zbierania informacji o celu
3.	Skanowanie podatności z wykorzystaniem Nessus, OpenVAS i innych skanerów - konfiguracja, uruchamianie skanów, analiza wyników
4.	Praktyczne ćwiczenia z testów penetracyjnych aplikacji webowych - identyfikacja i eksploatacja OWASP Top 10
5.	Ćwiczenia z testów infrastruktury - exploit lokalne i zdalne, eskalacja uprawnień, przemieszczanie się w sieci
6.	Symulowane kampanie phishingowe - przygotowanie, przeprowadzenie i analiza wyników ataków socjotechnicznych
7.	Bezpieczeństwo aplikacji mobilnych - testy aplikacji Android i iOS, analiza zabezpieczeń
8.	Dokumentacja przeprowadzonych działań - przygotowanie profesjonalnego raportu z testów penetracyjnych, kategoryzacja znalezisk
9.	Projekt zespołowy
10.	Projekt zespołowy
11.	Projekt zespołowy
12.	Projekt zespołowy
13.	Projekt zespołowy
14.	Prezentacje projektów zespołowych, omówienie znalezionych podatności, analiza skuteczności zastosowanych metod
15.	Prezentacje projektów zespołowych, omówienie znalezionych podatności, analiza skuteczności zastosowanych metod, wystawianie ocen
Metody dydaktyczne (realizacja stacjonarna)	W wykład problemowy; wykład z prezentacją multimedialną
	Ps programowanie z użyciem komputera
Metody dydaktyczne (realizacja zdalna)	W wykład z prezentacją multimedialną
	-
Forma zaliczenia	W zaliczenie pisemne
	Ps ocena sprawozdań z wykonanych zadań oraz ocena projektu
Warunki zaliczenia	Uzyskanie min. 30% punktów z każdego efektu uczenia się z zakresu wiedzy, a po spełnieniu tego warunku ostateczna ocena wynika z sumy uzyskanych punktów.
	Kryteria oceny: [0 - 50]% punktów - 2.0 (50 - 60)% punktów - 3.0 (60 - 70)% punktów - 3.5 (70 - 80)% punktów - 4.0 (80 - 90)% punktów - 4.5 (90 - 100)% punktów - 5.0
	Minimalne wymagania dotyczące poszczególnych efektów uczenia: E3 - przeprowadzenie podstawowych operacji w każdym etapie testów penetracyjnych w ramach realizowanego projektu E4 - uwzględnienie w raporcie z projektu dokumentacji z wykonanych czynności oraz przedstawienie podstawowych zaleceń dotyczących zabezpieczeń
	Ps Po spełnieniu powyższych warunków oraz zsumowaniu uzyskanych punktów: [0 - 50]% punktów - 2.0 (50 - 60)% punktów - 3.0 (60 - 70)% punktów - 3.5 (70 - 80)% punktów - 4.0 (80 - 90)% punktów - 4.5 (90 - 100)% punktów - 5.0

Symbol efektu	Zakładane efekty uczenia się	Odniesienie do efektów uczenia się zdefiniowanych dla kierunku studiów		
		Wiedza	Umiejętności	Kompetencje społeczne
Wiedza: student zna i rozumie				
E1	metodologie przeprowadzania testów penetracyjnych	INF1_W03 INF1_W08 INF1_W12 INF1_W14		
E2	metody i narzędzia stosowane do przeprowadzania testów penetracyjnych, w tym techniki socjotechniczne	INF1_W12 INF1_W14		
Umiejętności: student potrafi				
E3	przeprowadzać testy penetracyjne zgodnie w wybraną metodologią		INF1_U12 INF1_U13 INF1_U14	
E4	dokumentować wyniki przeprowadzonych testów oraz tworzyć zalecenia dotyczące zabezpieczeń		INF1_U07 INF1_U12 INF1_U17	

Symbol efektu	Sposób weryfikacji efektu uczenia się	Forma zajęć na której zachodzi weryfikacja
E1	zaliczenie pisemne	W
E2	zaliczenie pisemne	W
E3	ocena sprawozdań z wykonanych zadań, ocena projektu	Ps
E4	ocena sprawozdań z wykonanych zadań, ocena projektu	Ps
Literatura podstawowa	1. Kali Linux documentation - https://www.kali.org/docs	
	2. J. Arcuri, Warsztat Hakera: Testy penetracyjne i inne techniki wykrywania podatności, Helion, 2022	
	3. R. Messier, Kali Linux: Testy bezpieczeństwa, testy penetracyjne i etyczne hakowanie, Helion, 2019	
	4. Podręcznik systemowy GNU Linux	
Literatura uzupełniająca	1. K. Mitnick, Sztuka podstępów: łamałem ludzi, nie hasła, Helion, 2016	
	2. Netfilter, https://www.netfilter.org	
	3. Apache project, https://www.apache.org	
	4. Snort, https://www.snort.org	
	5. Suricata, https://suricata-ids.org	
Koordynator przedmiotu:	dr inż. Andrzej Chmielewski	Data: 02/03/2025

wydrukowane w programie **Świerk** , © Świerk V2