POLITECHNIKA BYDGOSKA
Wydział Inżynierii Mechanicznej

Karta przedmiotu

Zastosowanie i ochrona sieci komputerowych i bazy danych

1. Informacje podstawowe

Kierunek studiów technika bezpieczeństwa i obronności **Specjalność** - **Jednostka zarządzająca kierunkiem studiów** Wydział Inżynierii Mechanicznej **Poziom studiów** pierwszego stopnia (inż.) **Profil studiów** Profil ogólnoakademicki **Forma studiów** studia stacjonarne	**Cykl kształcenia (nabór)** 2024/25 **Kod przedmiotu** 03TBOS.PI2C.2874.24 **Języki wykładowe** polski **Obligatoryjność** Obowiązkowy **Blok zajęciowy** Przedmioty kierunkowe

Wymagania wstępne	
Przedmioty wprowadzające	
Koordynator	Krzysztof Nowicki

Okres	**Forma i godziny zajęć**	**Liczba punktów ECTS**
Semestr 2	• Wykład: 30, Zaliczenie na ocenę • Ćwiczenia laboratoryjne: 30, Zaliczenie na ocenę	5

2. Efekty uczenia się dla przedmiotu

Kod	**Opis efektów uczenia się**	**Odniesienie do kierunkowych efektów uczenia się**	**Odniesienie do charakterystyk PRK**
Wiedza:			

Kod	Opis efektów uczenia się	Odniesienie do kierunkowych efektów uczenia się	Odniesienie do charakterystyk PRK
W1	Student zna organizację i sposób funkcjonowania mechanizmów kontroli i sterowania przepływem danych w lokalnych sieciach komputerowych. Student posiada uporządkowaną wiedzę z zakresu planowania i budowania wielopoziomowych systemów bezpieczeństwa sieci lokalnych.	TBO_O1_K_W08, TBO_O1_K_W09	P6S_WG, P6S_WG_inż, P6S_WG P6S_WG_inż
Umiejętności:			
U1	Student potrafi przeprowadzić analizę przechwyconego ruchu danych przesyłanych w sieci lokalnej. Student potrafi zaprojektować rozwiązania służące do wielopoziomowego zabezpieczania lokalnych sieci komputerowych.	TBO_O1_K_U01, TBO_O1_K_U06	P6S_UW, P6S_UU, P6S_UW_inż, P6S_UW P6S_UW_inż
Kompetencje społeczne:			
K1	Student ma świadomość konieczności ustawicznego doskonalenia swojego stanu wiedzy z zakresu bezpieczeństwa sieci lokalnych, jak i nieustającego monitorowania wdrożonych systemów bezpieczeństwa.	TBO_O1_K_K05	P6S_KK

3. Treści programowe

Lp.	Treści programowe	Formy zajęć	Efekty uczenia się dla przedmiotu
1.	Polityka bezpieczeństwa. Bezpieczeństwo baz danych, uwierzytelnianie, kontrola dostępu, przetwarzanie transakcyjne, archiwizacja i odtwarzanie. Metody zarządzania dostępem do urządzeń i usług sieciowych. Wybrane podatności i zagrożenia w sieciach komputerowych. Wielopoziomowy system zabezpieczeń sieci komputerowych. Ataki na lokalne sieci bezprzewodowe oraz ich wykrywanie. Niesprawiedliwy dostęp do kanału radiowego. Beacon Flood. Authentication. Deauthentication. Fałszywy AP. Atak man-in-the-middle. RTS/CTS flood. ARP Poisoning. MAC Spoofing. Pozostałe ataki na sieci bezprzewodowe powodujące ich uszkodzenie. Bezprzewodowe sieci osobiste. Bezpieczeństwo transmisji w standardzie Bluetooth. Zarządzanie kluczem. Ataki na sieci Bluetooth: BLUEBug, BLUESnarf, BLUESnarf ++, BLUESmack, BLUEBump, BLUEDump, BLUEPrinting, BLUEChop, BLUEJacking. Profile Bluetooth. Omówienie wszystkich rozszerzeń standardu Bluetooth. 14. (90 min) Bezprzewodowe sieci osobiste. Omówienie bezpieczeństwa standardu ZigBee.	Wykład	W1, K1

Lp.	Treści programowe	Formy zajęć	Efekty uczenia się dla przedmiotu
2.	Zabezpieczanie dostępu do urządzeń sieciowych. Wybrane ataki w warstwie drugiej i trzeciej wraz z mechanizmami obrony. Przechwytywanie, zapisywanie, dekodowanie i analiza przesyłanych danych w sieci. Zaawansowane środowiska do przetwarzania i wspomagania procesu analizy logów generowanych przez urządzenia sieciowe. Analiza struktury ramek standardu IEEE 802.11 przy użyciu oprogramowania Wireshark. Analiza działania mechanizmu WPA/WPA2 i WPS. Zastosowanie tablic tęczowych. Tworzenie i konfiguracja wirtualnych sieci WLAN. Analiza działania standardu IEEE 802.1X oraz protokołów RADIUS i EAP. Analiza różnych typów ataków na sieci IEEE 802.11.	Ćwiczenia laboratoryjne	U1, K1

4. Metody prowadzenia zajęć, weryfikacji efektów uczenia się i warunki zaliczenia

Forma zajęć		
Wykład	**Metody prowadzenia zajęć:**	
	Wykład, Case study	
	Metody (sposoby) weryfikacji:	**Udział:**
	Zaliczenie pisemne	100%
	Warunki zaliczenia przedmiotu:	
	Minimum 50% z zaliczenia pisemnego.	
Ćwiczenia laboratoryjne	**Metody prowadzenia zajęć:**	
	Ćwiczenia laboratoryjne	
	Metody (sposoby) weryfikacji:	**Udział:**
	Raport	100%
	Warunki zaliczenia przedmiotu:	
	Przygotowanie raportów z ćwiczeń laboratoryjnych z wynikiem powyżej 2,95.	

Efekt uczenia się dla przedmiotu	**Metody (sposoby) weryfikacji**	
	Zaliczenie pisemne	Raport
W1	x	
U1		x
K1	x	x

5. Literatura

Literatura podstawowa

1. A.Silberschatz, H.F. Korth, S. Sudarshan,"Database System Concepts", McGrow Hill, 2019.
2. Lawrence C. Miller, Cybersecurity survival guide. Principles & Best Practices, Third Edition, August 2018
3. M. Gast: 802.11ac – A Survival Guide, 2013.

Literatura uzupełniająca

1. H.Garcia-Molina, J.Ullman, J.Widom "Database Systems The Complete Book", Prentice Hall, 2008. 2. D.Mendrala, M.Szeliga, Praktyczny kurs SQL. Wydanie III

6. Nakład pracy studenta - bilans godzin i punktów ECTS

Aktywność studenta		Obciążenie studenta Liczba godzin
Zajęcia prowadzone z bezpośrednim udziałem nauczyciela akademickiego lub innych osób prowadzących zajęcia	Wykład	30
	Ćwiczenia laboratoryjne	30
Praca własna studenta	Przygotowanie do zajęć	20
	Studiowanie literatury	25
	Konsultacje	10
	Inne (przygotowanie do egzaminu)	10
Łączny nakład pracy studenta		125
Liczba punktów ECTS		5

* Godzina (dydaktyczna) oznacza 45 minut