Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2019/2020

Wydział Informatyki i Telekomunikacji

Kierunek studiów: Informatyka | Profil: Ogólnoakademicki

Forma sudiów: stacjonarne | Kod kierunku: I

Stopień studiów: II

Specjalności: Cyberbezpieczeństwo dla licencjatów

1 Informacje o przedmiocie

Nazwa przedmiotu	Bezpieczeństwo w sieciach telekomunikacyjnych
Nazwa przedmiotu w języku angielskim	Security in telecommunications networks
Kod przedmiotu	WIiT I oIIS D4 19/20
Kategoria przedmiotu	Przedmioty specjalnościowe
Liczba punktów ECTS	4.00
Semestry	2

2 Rodzaj zajęć, liczba godzin w planie studiów

Semestr	Wykład	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Seminarium	Projekt
2	30	0	30	0	0	0

3 Cele przedmiotu

Cel 1 Wprowadzenie do bezpieczeństwa sieci telekomunikacyjnych

Cel 2 Zapoznanie studentów z metodami bezpiecznej transmisji przez sieć komputerową

4 Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1 znajomość podstaw sieci komputerowych (protokoły, techniki transmisji)

5 Efekty kształcenia

EK1 Umiejętności Student potrafi konfigurować sprzęt i oprogramowanie związane z bezpieczeństwem sieci.

EK2 Wiedza Student potrafi prezentować zagrożenia bezpieczeństwa w warstwach modeli OSI i TCP/IP.

EK3 Wiedza Student potrafi przedstawić metody bezpiecznej transmisji.

EK4 Wiedza Student potrafi przedstawić techniki ataków w sieciach komputerowych.

6 Treści programowe

Laboratorium		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
L1	Wykorzystanie sieci komputerowych	2
L2	Sniffing	2
L3	Wykrywanie sniffingu	2
L4	Scanning	2
L5	DoS/DDoS	2
L6	Ochrona przed DoS	2
L7	Man in the middle	2
L8	Bezpieczeństwo poczty elektronicznej	2
L9	VyOS	4
L10	Firewall programowe	2
L11	Firewall sprzętowe	4
L12	Hasła i funkcje skrótu	2
L13	Kali Linux	2

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W1	transmisja w sieci komputerowej i techniki ataków	4

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W2	Bezpieczeństwo w warstwie alpikacji	4
W3	Bezpieczeństwo w warstwie transportowej	2
W4	Bezpieczeństwo w warstwie sieci	2
W5	Bezpieczeństwo w warstwie łącza danych	2
W6	Bezpieczeństwo w warstwie fizycznej	2
W7	transmisja bezprzewodowa i zagrożenia	2
W8	VPN	2
W9	Firewall	2
W10	Testy penetracyjne	3
W11	ACL	2
W12	AAA	2
W13	Certyfikaty	1

7 Narzędzia dydaktyczne

N1 Wykłady

N2 Ćwiczenia laboratoryjne

N3 Dyskusja

N4 Konsultacje

8 Obciążenie pracą studenta

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z nauczycielem akademickim, w tym:	
Godziny wynikające z planu studiów	60
Konsultacje przedmiotowe	4
Egzaminy i zaliczenia w sesji	4
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	30
Opracowanie wyników	30
Przygotowanie raportu, projektu, prezentacji, dyskusji	30
Sumaryczna liczba godzin dla przedmiotu wynikająca z całego nakładu pracy studenta	**158**
Sumaryczna liczba punktów ECTS dla przedmiotu	4.00

9 Sposoby oceny

Ocena formująca

F1 Kolokwium

F2 Test

F3 Sprawozdania z ćwiczeń laboratoryjnych

Ocena podsumowująca

P1 Egzamin pisemny

P2 Średnia ważona ocen formujących

Warunki zaliczenia przedmiotu

W1 Pozytywną ocenę mogą uzyskać studenci, którzy regularnie uczęszczali do laboratoriów.

W2 Konieczność zaliczenia wszystkich testów i ćwiczeń praktycznych przed przystąpieniem do egzaminu.

Ocena aktywności bez udziału nauczyciela

B1 Ocena ze sprawozdania laboratoryjnego przygotowanego przez studenta

Kryteria oceny

Efekt kształcenia 1	
Na ocenę 2.0	Student nie potrafi przeprowadzić konfiguracji.
Na ocenę 3.0	Student potrafi wykonać częściową konfigurację, często popełniając błędy.
Na ocenę 3.5	Student potrafi konfigurować podstawowe usługi, błędy popełnia rzadko.
Na ocenę 4.0	Student potrafi konfigurować zaawansowane metody bezpieczeństwa, ma odpowiednią wiedzę, zaawansowana konfiguracja nie zawsze działa poprawnie.
Na ocenę 4.5	Student radzi sobie z konfiguracją zaawansowanych metod bezpieczeństwa, ma szeroki zakres wiedzy pozwalający mu zrozumieć konfigurowane metody.
Na ocenę 5.0	Student radzi sobie z konfiguracją każdej podstawowej i zaawansowanej usługi bezpieczeństwa.
Efekt kształcenia 2	
Na ocenę 2.0	Student nie potrafi wymienić podstawowych metod bezpiecznej transmisji danych.
Na ocenę 3.0	Student potrafi opisać podstawowe metody bezpiecznej transmisji danych. Student zna model OSI.
Na ocenę 3.5	Student zna model OSI i TCP/IP. Student potrafi w prosty sposób przypisywać techniki ataku do warstw modelu.
Na ocenę 4.0	Student potrafi szczegółowo opisać techniki ataków i podstawowo techniki obrony.
Na ocenę 4.5	Student potrafi szczegółowo opisać techniki obrony przed atakami w sieci.
Na ocenę 5.0	Student zna wszystkie techniki ataku i metody obrony przed nimi przy użyciu zaawansowanych narzędzi.
Efekt kształcenia 3	
Na ocenę 2.0	Student nie potrafi wymieniać podstawowych metod bezpiecznej transmisji danych.
Na ocenę 3.0	Student potrafi opisać podstawowe metody zabezpieczania sieci komputerowych.
Na ocenę 3.5	Student potrafi szczegółowo opisać metody bezpiecznej transmisji danych.
Na ocenę 4.0	Student potrafi opisać zasady VPN, ACL, AAA i sposoby ich konfiguracji.
Na ocenę 4.5	Student zna wszystkie techniki bezpiecznej transmisji danych i potrafi je skonfigurować.
Na ocenę 5.0	Student potrafi konfigurować zaawansowane narzędzia bezpieczeństwa i ma szeroką wiedzę na temat bezpiecznej transmisji danych.
Efekt kształcenia 4	

Na ocenę 2.0	Student nie potrafi wymienić podstawowych metod bezpiecznej transmisji danych.
Na ocenę 3.0	Student potrafi opisać podstawowe metody bezpiecznej transmisji danych.
Na ocenę 3.5	Student potrafi wymienić i opisać techniki ataków pasywnych.
Na ocenę 4.0	Student potrafi wymienić i opisać techniki aktywnych ataków.
Na ocenę 4.5	Student zna metody obrony przed atakami pasywnymi i aktywnymi.
Na ocenę 5.0	Student ma szeroką wiedzę i potrafi konfigurować zaawansowane narzędzia bezpieczeństwa.

10 Macierz realizacji przedmiotu

Efekt kształcenia	Odniesienie danego efektu do szczegółowych efektów zdefiniowanych dla programu	Cele przedmiotu	Treści programowe	Narzędzia dydaktyczne	Sposoby oceny
EK1	I2_W02 I2_W06 I2_U03b	Cel 1	L6 L9 L10 L11 L13 W9 W10 W11 W12	N1 N2 N3 N4	F1 F2 F3 P1 P2
EK2	I2_W06 I2_U06 I2_K04	Cel 2	L1 L2 L3 L4 L5 L6 L7 W2 W3 W4 W5 W6 W7	N1 N2 N3 N4	F1 F2 F3 P1 P2
EK3	I2_W02 I2_K04	Cel 1	L10 L11 L12 W1 W8 W13	N1 N2 N3 N4	F1 F2 F3 P1 P2
EK4	I2_W02 I2_W06 I2_U07	Cel 2	L1 L2 L3 L4 L5 L6 L7 L8 W2 W3 W4 W5 W6 W7	N1 N2 N3 N4	F1 F2 F3 P1 P2

11 Wykaz literatury

Literatura podstawowa

[1] William Stallings, Lawrie Brown — *Bezpieczeństwo systemów informatycznych. Zasady i praktyka.*, , 2016, Helion

[2] Chris McNab — *Network Security Assessment*, , 2016, O'Reilly Media

[3] WatchGuard — *WatchGuardhttp://www.watchguard.com/help/docs/webui/XTM_ 11/en-US/v11_ 9_ Web_ UI_ User_ Gui US).pdf*, , 2014,

[4] Michal Zalewski — *Cisza w sieci*, , 2005, Helion

[6] — *Źródła internetowe (Sekurak, Haking)*, , 0,

Literatura uzupełniająca

[1] Adam Józefiok — *Security CCNA 210-260. Zostań administratorem sieci komputerowych Cisco*, , 2016, Helion

12 Informacje o nauczycielach akademickich

Osoba odpowiedzialna za kartę

dr inż. Dariusz Żelasko (kontakt: `dzelasko@pk.edu.pl`)

Osoby prowadzące przedmiot

1 mgr inż. Dariusz Żelasko (kontakt: `dzelasko@pk.edu.pl`)

13 Zatwierdzenie karty przedmiotu do realizacji

(miejscowość, data) (odpowiedzialny za przedmiot) (dziekan)

Przyjmuję do realizacji (data i podpisy osób prowadzących przedmiot)

. . . . . .