Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2017/2018

Wydział Fizyki, Matematyki i Informatyki

Kierunek studiów: Informatyka

Profil: Ogólnoakademicki

Forma sudiów: stacjonarne

Kod kierunku: I

Stopień studiów: II

Specjalności: Teleinformatyka dla licencjatów

1 Informacje o przedmiocie

Nazwa przedmiotu	Bezpieczeństwo systemów teleinformatycznych
Nazwa przedmiotu w języku angielskim	Security of ICT systems
Kod przedmiotu	WFMiI I oIIS D8 17/18
Kategoria przedmiotu	Przedmioty specjalnościowe
Liczba punktów ECTS	4.00
Semestry	4

2 Rodzaj zajęć, liczba godzin w planie studiów

Semestr	Wykład	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Seminarium	Projekt
4	30	0	30	0	0	0

3 Cele przedmiotu

Cel 1 Poszerzenie wiedzy studenta z zakresu bezpieczeństwa systemów teleinformatycznych zdobytą na przedmiocie bezpieczeństwo systemów komputerowych.

Cel 2 Zapoznanie studentów z wybranymi technikami i rozwiązaniami, których zadaniem jest zapewnienie bezpiecznej komunikacji w sieciach teleinformatycznych.

Cel 3 Zapoznanie studentów z wybranymi protokołami sieciowymi gwarantującymi bezpieczeństwo transmisji danych w systemach teleinformatycznych.

Cel 4 Zapoznanie studentów z podstawowymi technikami testowania zabezpieczeń systemów teleinformatycznych.

4 Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1 Zaliczenie przedmiotu sieci komputerowe.

2 Zaliczenie przedmiotu bezpieczeństwo systemów komputerowych.

5 Efekty kształcenia

EK1 Wiedza Student zna i potrafi omówić techniki odzyskiwania plików, zagadnienia bezpieczeństwa aplikacji mobilnych, .NET i aplikacji internetowych, zagadnienia cyberbezpieczeństwa i chmury obliczeniowej, podstawowe techniki biometryczne.

EK2 Umiejętności Student potrafi konfigurować urządzenia klasy SSL VPN Gateway.

EK3 Umiejętności Student potrafi przedstawić i omówić podstawowe techniki przeprowadzania testów zabezpieczeń systemów teleinformatycznych.

EK4 Kompetencje społeczne Umie - zgodnie z zadaną specyfikacją - zaprojektować oraz zrealizować prosty system informatyczny, używając właściwych metod, technik i narzędzi.

6 Treści programowe

Laboratorium		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
L1	Bezpieczeństwo i odzyskiwanie danych	4
L2	Bezpieczeństwo aplikacji mobilnych, .NET i internetowych	4
L3	Cyberbezpieczeństwo	4
L4	Bezpieczeństwo chmury obliczeniowej	2
L5	Biometria	4
L6	Podstawowe techniki zbierania informacji o systemach teleinformatycznych	4
L7	Testowanie zabezpieczeń systemów teleinformatycznych	4
L8	Bezpieczeństwo serwera sieciowego	4

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W2	Bezpieczeństwo i odzyskiwanie danych	4
W3	Bezpieczeństwo aplikacji mobilnych, .NET i internetowych	4
W5	Cyberbezpieczeństwo	4
W7	Bezpieczeństwo chmury obliczeniowej	2
W8	Biometria	4
W9	Omówienie podstawowych technik zbierania informacji o systemach teleinformatycznych.	4
W10	Omówienie technik testowania zabezpieczeń systemów teleinformatycznych.	4
W11	Bezpieczeństwo serwera sieciowego.	4

7 Narzędzia dydaktyczne

N1 Wykłady

N2 Ćwiczenia laboratoryjne

N3 Prezentacje multimedialne

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	0
Egzaminy i zaliczenia w sesji	0
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	60
Opracowanie wyników	0
Przygotowanie raportu, projektu, prezentacji, dyskusji	0
Sumaryczna liczba godzin dla przedmiotu wynikająca z całego nakładu pracy studenta	**120**
Sumaryczna liczba punktów ECTS dla przedmiotu	4.00

9 Sposoby oceny

Ocena formująca

F1 Ćwiczenie praktyczne

F2 Kolokwium

Ocena podsumowująca

P1 Egzamin pisemny

P2 Średnia ważona ocen formujących

Warunki zaliczenia przedmiotu

W1 Konieczność zaliczenia wszystkich kolokwiów oraz ćwiczenia praktycznego przed przystąpieniem do egzaminu.

Kryteria oceny

Efekt kształcenia 1	
Na ocenę 2.0	Student nie potrafi konfigurować zaawansowanych funkcjonalności bezpieczeństwa dla urządzeń klasy XTM.
Na ocenę 3.0	Student potrafi integrować urządzenie klasy XTM z zewnętrzną bazą autentykacji.

Na ocenę 3.5	Student potrafi konfigurować funkcjonalność SSO dla urządzeń klasy XTM.
Na ocenę 4.0	Student potrafi konfigurować filtr ochrony antyspamowej w urządzeniach klasy XTM.
Na ocenę 4.5	Student potrafi konfigurować filtr ochrony przed intruzami w urządzeniach klasy XTM.
Na ocenę 5.0	Student potrafi testować jakość ochrony realizowanej przez urządzenie klasy XTM.
Efekt kształcenia 2	
Na ocenę 2.0	Student nie potrafi konfigurować podstawowych funkcjonalności urządzeń klasy SSL VPN Gateway.
Na ocenę 3.0	Student nie potrafi konfigurować podstawowe funkcjonalności urządzeń klasy SSL VPN Gateway.
Na ocenę 3.5	Student potrafi integrować urządzenie SSL VPN Gateway z zewnętrzną bazą autentykacji.
Na ocenę 4.0	Student potrafi konfigurować wszystkie typy autentykacji dostępne w urządzeniu SSL VPN Gateway. Student potrafi tworzyć nowe zasoby.
Na ocenę 4.5	Student potrafi konfigurować reguły dostępu do zasobów obejmujące weryfikacje zabezpieczeń systemu operacyjnego, z którego następuje połączenie oraz usuwanie wszelkich danych po zakończonej sesji użytkownika.
Na ocenę 5.0	Student potrafi personalizować portal z zasobami oraz analizować logi i generować raporty aktywności.
Efekt kształcenia 3	
Na ocenę 2.0	Student nie potrafi wymienić podstawowych protokołów sieciowych gwarantujących bezpieczeństwo transmisji danych w systemach teleinformatycznych.
Na ocenę 3.0	Student potrafi wymienić podstawowe protokoły sieciowe gwarantujące bezpieczeństwo transmisji danych w systemach teleinformatycznych.
Na ocenę 3.5	Student potrafi wskazać zmiany wprowadzone w bezpiecznych protokołach względem standardowych protokołów i uzasadnić ich znaczenie dla bezpieczeństwa transmisji w systemach teleinformatycznych.
Na ocenę 4.0	Student potrafi zaprezentować zasadę działania protokołu DNSSec.
Na ocenę 4.5	Student potrafi przedstawić zasadę działania protokołu SSL.
Na ocenę 5.0	Student potrafi ze szczegółami omówić proces nawiązywania połączenia SSL.
Efekt kształcenia 4	
Na ocenę 2.0	Student nie potrafi wymienić podstawowych technik przeprowadzania testów zabezpieczeń systemów teleinformatycznych.

Na ocenę 3.0	Student potrafi wymienić podstawowe techniki przeprowadzania testów zabezpieczeń systemów teleinformatycznych.
Na ocenę 3.5	Student potrafi zaprezentować podstawowe techniki zbierania informacji o systemach teleinformatycznych.
Na ocenę 4.0	Student potrafi zaprezentować techniki łamania haseł.
Na ocenę 4.5	Student potrafi omówić podstawowe narzędzia i techniki weryfikowania zabezpieczeń usług sieciowych.
Na ocenę 5.0	Student potrafi omówić zastosowanie narzędzi zgromadzonych w ramach dystrybucji BackTrack.

10 Macierz realizacji przedmiotu

Efekt kształcenia	Odniesienie danego efektu do szczegółowych efektów zdefiniowanych dla programu	Cele przedmiotu	Treści programowe	Narzędzia dydaktyczne	Sposoby oceny
EK1		Cel 1	W2 W3 W5 W7 W8 W9 W10 W11	N1 N3 N4	F1 F2 P1 P2
EK2		Cel 2	L1 L2 L3 L4 L5 L6 L7 L8	N1 N2 N3 N4	F1 F2 P1 P2
EK3		Cel 3	L1 L2 L3 L4 L5 L6 L7 L8	N1 N3 N4	F2 P1
EK4		Cel 2 Cel 3	L1 L2 L3 L4 L5 L6 L7 L8	N2 N3 N4	F1

11 Wykaz literatury

Literatura podstawowa

[1] RFC — *Dokumenty RFC dla DNSSec, SSL.*, RFC, 2011, RFC

[2] Honeypots.net — *http://www.honeypots.net/*, www, 2011, Honeypots.net

[3] Dnssec.net — *http://www.dnssec.net/*, www, 2011, Dnssec.net

[4] Sourcefire — *http://www.snort.org/*, www, 2011, Sourcefire

[5] Michał Piotrowski — *Królicza nora : ochrona sieci komputerowych za pomocą technologii honeypot*, Warszawa, 2007, PWN

[6] Rolf Oppliger — *SSL and TLS Theory and Practice*, Norwood, 2009, Artech House

[7] Bauer, Michael D. — *Linux : serwery : bezpieczeństwo : kompendium wiedzy o ochronie serwerów linuksowych przed atakami z sieci*, Gliwice, 2005, Helion

Literatura uzupełniająca

[1] Alex Lukatsky — *Wykrywanie włamań i aktywna ochrona danych : elita rosyjskich hakerów prezentuje*, Gliwice, 2005, Helion

[2] Łuczak Jacek — *Zarządzanie bezpieczeństwem informacji : praca zbiorowa / Jacek Łuczak (red.)*, Poznań, 2004, Oficyna Współczesna

12 Informacje o nauczycielach akademickich

Osoba odpowiedzialna za kartę

dr inż. Krzysztof Rzecki (kontakt: krz@pk.edu.pl)

Osoby prowadzące przedmiot

1 mgr inż. Tomasz Sośnicki (kontakt: tsosnicki@pk.edu.pl)

2 dr inż. Krzysztof Rzecki (kontakt: krz@itt.pk.edu.pl)

13 Zatwierdzenie karty przedmiotu do realizacji

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

Przyjmuję do realizacji (data i podpisy osób prowadzących przedmiot)

. . . . . .

. . . . . .