Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2012/2013

Wydział Fizyki, Matematyki i Informatyki

Kierunek studiów: Informatyka

Profil: Ogólnoakademicki

Forma sudiów: stacjonarne

Kod kierunku: I

Stopień studiów: I

Specjalności: Brak specjalności

1 Informacje o przedmiocie

Nazwa przedmiotu	Bezpieczeństwo systemów komputerowych
Nazwa przedmiotu w języku angielskim	
Kod przedmiotu	WFMiI I oIS D1 12/13
Kategoria przedmiotu	Przedmioty specjalnościowe
Liczba punktów ECTS	5.00
Semestry	6

2 Rodzaj zajęć, liczba godzin w planie studiów

Semestr	Wykład	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Seminarium	Projekt
6	30	0	30	0	0	0

3 Cele przedmiotu

Cel 1 Wprowadzenie w tematykę bezpieczeństwa systemów komputerowych.

Cel 2 Zapoznanie z tematyką zabezpieczania przesyłania informacji.

Cel 3 Zapoznanie studentów z metodami bezpiecznego łączenia geograficznie rozproszonych lokalizacji w logiczną wirtualną sieć.

Cel 4 Zapoznanie studentów z metodami zapewniania bezpiecznego zdalnego dostępu do zasobów sieci chronionej.

Cel 5 Zapoznanie studentów z technikami filtrowania ruchu sieciowego w warstwach od 3 wzwyż siedmiowarstwowego modelu sieci.

Cel 6 Zapoznanie studentów ze sposobami konfigurowania filtrów pakietów oraz proxy filtrujących.

Cel 7 Prezentacja metod realizacji redundancji systemów zabezpieczeń sieciowych.

4 Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1 Znajomość podstawowych protokołów sieciowych (m.in. Ethernet, ARP, RARP, ICMP, IP, TCP, UDP, DNS, HTTP, SMTP) i zasad działania sieci komputerowych.

2 Zaliczenie przedmiotu sieci komputerowe.

5 Efekty kształcenia

EK1 Umiejętności Student potrafi konfigurować zintegrowane sprzętowe urządzenia zabezpieczające sieć klasy XTM.

EK2 Wiedza Student potrafi przedstawić zasadę działania podstawowych metod zabezpieczania systemów komputerowych.

EK3 Wiedza Student potrafi przedstawić podstawowe metody bezpiecznej transmisji danych.

EK4 Wiedza Student potrafi przedstawić podstawowe zagrożenia systemów komputerowych.

6 Treści programowe

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W1	Wstęp, omówienie zasad zaliczenia, prezentacja wykorzystywanych na laboratorium urządzeń.	2
W2	Przedstawienie aktualnych trendów w bezpieczeństwie i ostatnio zidentyfikowanych zagrożeń.	2
W3	Aspekty bezpieczeństwa systemów informatycznych.	4
W4	Realizacja usług zapewnienia bezpieczeństwa informacji.	2
W5	Podstawowe typy i własności systemów kryptograficznych.	4
W6	Infrastruktura Klucza Publicznego PKI.	2
W7	Zagrożenia zewnętrzne.	2
W8	Systemy wykrywania włamań (IDS).	2
W9	Protokół IPSec.	2

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W10	Prywatność w ruchu sieciowym.	2
W11	Ukrywanie ruchu steganografia sieciowa.	2
W12	Monitorowanie ruchu sieciowego w celu zapewnienia bezpieczeństwa.	2
W13	Bezpieczeństwo sieci bezprzewodowych.	2

Laboratorium		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
L1	Quick Setup Wizard wstępna konfiguracja urządzeń klasy XTM.	2
L2	Konfiguracja filtrów pakietów.	2
L3	Konfiguracja Proxy filtrujących.	2
L4	Centralne zarządzanie wieloma urządzeniami.	2
L5	Autentykacja użytkowników, tworzenie polityk bezpieczeństwa bazujących na tożsamości użytkowników.	2
L6	Generowanie, magazynowanie, przeglądanie logów, generowanie raportów.	2
L7	Konfigurowanie tuneli VPN dla użytkowników mobilnych z wykorzystaniem PPTP oraz SSL.	2
L8	Konfigurowanie tuneli VPN dla użytkowników mobilnych z wykorzystaniem IPSec.	2
L9	Konfigurowanie statycznych tuneli VPN pomiędzy urządzeniami.	2
L10	Obsługa wielu łączy zewnętrznych MultiWAN.	2
L11	Klastrowanie urządzeń (Fire Cluster).	2
L12	Filtrowanie zawartości stron www (WebBlocker).	2
L13	Konfigurowanie modułu ochrony przed intruzami (IPS).	2
L14	Filtrowanie aplikacji generujących ruch sieciowy (Application control).	2
L15	Sprawdzian umiejętności konfigurowania urządzeń klasy XTM.	2

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	0
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	90
Opracowanie wyników	0
Przygotowanie raportu, projektu, prezentacji, dyskusji	0
Sumaryczna liczba godzin dla przedmiotu wynikająca z całego nakładu pracy studenta	**90**
Sumaryczna liczba punktów ECTS dla przedmiotu	5.00

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 podstawowych ustawień sieciowych urządzeń klasy XTM. Student nie potrafi konfigurować filtrów pakietów.
Na ocenę 3.0	Student potrafi konfigurować podstawowe ustawienia sieciowe urządzeń klasy XTM. Student potrafi konfigurować filtry pakietów.
Na ocenę 3.5	Student potrafi konfigurować proxy filtrujące dla protokołów HTTP, HTTPS, DNS, FTP.
Na ocenę 4.0	Student potrafi konfigurować tunele VPN, zarówno statyczne jak i mobilne. Student potrafi analizować zebrane logi oraz generować raporty aktywności użytkowników.
Na ocenę 4.5	Student potrafi konfigurować polityki bezpieczeństwa bazujące na tożsamości użytkowników. Student potrafi konfigurować zaawansowane ustawienia sieciowe urządzeń.
Na ocenę 5.0	Student potrafi konfigurować dodatkowe usługi bezpieczeństwa: ochrona przed spamem, IPS, ochrona antywirusowa, Application Control, filtrowanie zawartości stron www. Student potrafi klastrować urządzenia.
Efekt kształcenia 2	
Na ocenę 2.0	Student nie potrafi wymienić podstawowych metod zabezpieczania systemów komputerowych.
Na ocenę 3.0	Student potrafi wymienić podstawowe metody zabezpieczania systemów komputerowych.
Na ocenę 3.5	Student potrafi opisać zasadę działania zapory sieciowej, potrafi zaprezentować różnice pomiędzy poszczególnymi typami zapór sieciowych.
Na ocenę 4.0	Student potrafi zaprezentować zasadę działania oraz typy systemów ochrony przed intruzami (IDS).
Na ocenę 4.5	Student potrafi przedstawić typy ochrony antyspamowej oraz opisać ich zasadę działania.
Na ocenę 5.0	Student potrafi opisać zasadę działania Proxy filtrujących.
Efekt kształcenia 3	
Na ocenę 2.0	Student nie potrafi wymienić podstawowych metod bezpiecznej transmisji danych.
Na ocenę 3.0	Student potrafi wymienić podstawowe metody bezpiecznej transmisji danych.
Na ocenę 3.5	Student potrafi porównać zalety poszczególnych metod bezpiecznej transmisji danych.
Na ocenę 4.0	Student potrafi opisać zasadę działania protokołu IPSec.
Na ocenę 4.5	Student potrafi opisać zasadę działania, przedstawić strukturę oraz zależności pomiędzy elementami infrastruktury PKI.
Na ocenę 5.0	Student potrafi opisać zasady ukrywania ruchu sieciowego w innych protokołach.

Efekt kształcenia 4	
Na ocenę 2.0	Student nie potrafi wymienić podstawowych zagrożeń systemów komputerowych.
Na ocenę 3.0	Student potrafi wymienić podstawowe zagrożenia systemów komputerowych.
Na ocenę 3.5	Student potrafi porównać poziom niebezpieczeństwa podstawowych zagrożeń systemów komputerowych.
Na ocenę 4.0	Student potrafi opisać i porównać różne typy ataków DoS.
Na ocenę 4.5	Student potrafi opisać istotę i zasadę przeprowadzania ataków typu APT.
Na ocenę 5.0	Student potrafi przedstawić podstawowe ataki kierowane przeciwko sieci Web.

10 Macierz realizacji przedmiotu

Efekt kształcenia	Odniesienie danego efektu do szczegółowych efektów zdefiniowanych dla programu	Cele przedmiotu	Treści programowe	Narzędzia dydaktyczne	Sposoby oceny
EK1	I1_U15 I1_U16 I1_U22 I1_U24	Cel 3 Cel 5 Cel 6 Cel 7	W1 L1 L2 L3 L4 L5 L6 L7 L8 L9 L10 L11 L12 L13 L14 L15	N1 N2 N3 N4	F1 P2
EK2	I1_W05	Cel 2	W3 W4 W5 W6 W8 W10	N1 N2 N3 N4	F2 P1 P2
EK3	I1_W11	Cel 4	W9 W10 W11 W12 W13	N1 N2 N3 N4	F2 P1 P2
EK4	I1_W14	Cel 1	W2 W3 W7 W11 W13	N1 N3 N4	F2 P1 P2

11 Wykaz literatury

Literatura podstawowa

[1] WatchGuard — *http://www.watchguard.com/help/docs/wsm/11/en-US/index.html*, www, 2011, WatchGuard

[2] Steve Friedl — *http://unixwiz.net/techtips/iguide-ipsec.ht*, www, 2005, Steve Friedl

[3] Karen Scarfone, Peter Mell — *http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf*, www, 2007, National Institute of Standards and Technology

[4] Carlisle Adams, Steve Lloyd — *PKI podstawy i zasady działania : koncepcje, standardy i wdrażanie infrastruktury kluczy publicznych*, Warszawa, 2007, PWN

12 Informacje o nauczycielach akademickich

Osoba odpowiedzialna za kartę

Marcin Klamra (kontakt: mklamra@l5.pk.edu.pl)

Osoby prowadzące przedmiot

1 mgr inż. Marcin Klamra (kontakt: mklamra@iti.pk.edu.pl)

2 mgr inż. Tomasz Sośnicki (kontakt: tom.sosnicki@gmail.com)

13 Zatwierdzenie karty przedmiotu do realizacji

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

Przyjmuję do realizacji (data i podpisy osób prowadzących przedmiot)

. . . . . .

. . . . . .