Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2018/2019

Wydział Mechaniczny

Kierunek studiów: Informatyka Stosowana

Profil: Ogólnoakademicki

Forma sudiów: stacjonarne

Kod kierunku: S

Stopień studiów: I

Specjalności: Informatyka Stosowana

1 Informacje o przedmiocie

Nazwa przedmiotu	Administracja i bezpieczeństwo systemów komputerowych
Nazwa przedmiotu w języku angielskim	Computer systems administration and security
Kod przedmiotu	WM INFST oIS C15 18/19
Kategoria przedmiotu	Przedmioty kierunkowe
Liczba punktów ECTS	4.00
Semestry	6

2 Rodzaj zajęć, liczba godzin w planie studiów

Semestr	Wykład	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Projekt	Seminarium
6	15	0	30	0	15	0

3 Cele przedmiotu

Cel 1 Zapoznanie się z narzędziami do administracji systemów komputerowych, poznanie źródeł zagrożeń dla ich bezpieczeństwa oraz metod ochrony przed nimi. Zdobycie umiejętności administracji systemem serwera oraz bezpieczeństwem systemów komputerowych na przykładzie systemów MS Windows Server oraz Unix/Linux.

4 Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1 Brak wymagań.

5 Efekty kształcenia

EK1 Wiedza Zna systemy serwerów sieciowych na poziomie administracyjnym oraz usługi serwerowe dla użytkowników sieci lokalnej i w Internecie. Zna zagadnienia ich niezawodności, zapewnienia wydajności oraz bezpieczeństwa.

EK2 Wiedza Zna metody projektowania i implementacji infrastruktury systemów informatycznych oraz procedury administrowania usługami sieciowymi oraz zapewnienia wymaganego stopnia bezpieczeństwa.

EK3 Umiejętności Potrafi zaprojektować zgodnie ze specyfikacją infrastrukturę sieciowego systemu informatycznego oraz systemu zapewnienia bezpieczeństwa.

EK4 Umiejętności Potrafi zaplanować i nadzorować zadania obsługowe dla zapewnienia niezawodnej eksploatacji systemów operacyjnych serwerów sieciowych oraz bezpieczeństwa informatycznego infrastruktury.

6 Treści programowe

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W1	Administracja systemami serwerowymi UNIX, administracja usługami oraz zasobami (DHCP, DNS, SMTP, kopie bezpieczeństwa, zarządzania użytkownikami).	7
W2	Problemy bezpieczeństwa w systemach i sieciach komputerowych co chronić, przed czym chronić, podstawowe typy ataków: Sniffing, ARP Spoofing, IP Spoofing, DoS. Metody przeciwdziałania atakom, założenia projektowe bezpiecznych systemów komputerowych (zarządzanie ryzykiem).	2
W3	Podstawy kryptografii: szyfry proste, szyfry komputerowe symetryczne i niesymetryczne. Algorytmy DES, IDEA, AES, RSA. Protokoły wymiany klucza, funkcje skrótu MD5, SHA. Infrastruktura klucza publicznego podpis elektroniczny w świetle przepisów, zarządzanie kluczami publicznymi uwierzytelnianie z wykorzystaniem algorytmów niesymetrycznych.	2
W4	Zarządzanie bezpieczeństwem infrastruktury zabezpieczenia stosowane w transmisji danych technologie VPN, SSL, SSH, KERBEROS. Bezpieczeństwo sieci bezprzewodowych. Metody wykrywania ataków na infrastrukturę (IDS, IPS, Firewall). Wirusy, konie trojańskie, programy szpiegujące możliwe drogi infekcji, metody przeciwdziałania.	4

Projekt		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin

Projekt		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
P1	Projekt infrastruktury serwerów usługowych dla sieci lokalnej małego i średniego przedsiębiorstwa w oparciu o rozwiązania MS Windows Server wg specfikacji.	5
P2	Projekt infrastruktury serwerów usług sieciowych w Internecie z uwzględnieniem niezawodności i bezpieczeństwa wg podanej specyfikacji.	5
P3	Projekt systemu zapewnienia bezpieczeństwa infrastruktury i zasobów sieci wg specyfikacji.	5

Laboratorium		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
L1	Administracja systemami MS Windows oraz Linux (PAM, LDAP, rozszerzone listy ACL, usługi serwerowe, usługi katalogowe).	16
L2	Narzędzia do analizy ruchu sieciowego oraz wykrywania ataków (Ethereal, SNORT). Kryptografia analiza algorytmów (Cryptool). Zastosowanie PKI w podpisie elektronicznym.	8
L3	Tunelowanie transmisji prywatne sieci wirtualne VPN. Budowa i zarządzanie systemów zapory ogniowej firewall programowy oraz sprzętowy.	6

7 Narzędzia dydaktyczne

N1 Wykłady

N2 Ćwiczenia laboratoryjne

N3 Ćwiczenia projektowe

N4 Praca w grupach

N5 Prezentacje multimedialne

N6 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	5
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	30
Opracowanie wyników	0
Przygotowanie raportu, projektu, prezentacji, dyskusji	55
Sumaryczna liczba godzin dla przedmiotu wynikająca z całego nakładu pracy studenta	**150**
Sumaryczna liczba punktów ECTS dla przedmiotu	4.00

9 Sposoby oceny

Ocena formująca

F1 Ćwiczenie praktyczne

F2 Projekt indywidualny

F3 Projekt zespołowy

F4 Test

Ocena podsumowująca

P1 Średnia ważona ocen formujących

Ocena aktywności bez udziału nauczyciela

B1 Ćwiczenie praktyczne

B2 Projekt indywidualny

B3 Projekt zespołowy

B4 Test

Kryteria oceny

Efekt kształcenia 1

Na ocenę 2.0	-
Na ocenę 3.0	Potrafi zastosować do określonych wymagań odpowiednie rozwiązanie techniczne dla infrastruktury serwerowej systemu informatycznego oraz w zakresie bezpieczeństwa pojedynczego komputera, infrastruktury sieci oraz transmisji danych w sieci publicznej.
Na ocenę 3.5	-
Na ocenę 4.0	-
Na ocenę 4.5	-
Na ocenę 5.0	-
Efekt kształcenia 2	
Na ocenę 2.0	-
Na ocenę 3.0	jw.
Na ocenę 3.5	-
Na ocenę 4.0	-
Na ocenę 4.5	-
Na ocenę 5.0	-
Efekt kształcenia 3	
Na ocenę 2.0	-
Na ocenę 3.0	jw.
Na ocenę 3.5	-
Na ocenę 4.0	-
Na ocenę 4.5	-
Na ocenę 5.0	-
Efekt kształcenia 4	
Na ocenę 2.0	-
Na ocenę 3.0	jw.
Na ocenę 3.5	-
Na ocenę 4.0	-
Na ocenę 4.5	-
Na ocenę 5.0	-

10 Macierz realizacji przedmiotu

Efekt kształcenia	Odniesienie danego efektu do szczegółowych efektów zdefiniowanych dla programu	Cele przedmiotu	Treści programowe	Narzędzia dydaktyczne	Sposoby oceny
EK1	K1_W10	Cel 1	W1 W2 W3 W4 P1 P2 P3 L1 L2 L3	N1 N2 N3 N4 N5 N6	F1 F2 F3 F4 P1
EK2	K1_W12	Cel 1	W1 W2 W3 W4 P1 P2 P3 L1 L2 L3	N1 N2 N3 N4 N5 N6	F1 F2 F3 F4 P1
EK3	K1_UB08	Cel 1	W1 W2 W3 W4 P1 P2 P3 L1 L2 L3	N1 N2 N3 N4 N5 N6	F1 F2 F3 F4 P1
EK4	K1_UB09	Cel 1	W1 W2 W3 W4 P1 P2 P3 L1 L2 L3	N1 N2 N3 N4 N5 N6	F1 F2 F3 F4 P1

11 Wykaz literatury

Literatura podstawowa

[1] Garfinkel S. i Spafford G. — *Bezpieczeństwo w Unixie i Internecie*, Warszawa, 2003, Wydawnictwo RM

[2] Stokłosa J., Bliski T., Pankowski T. — *Bezpieczeństwo danych w systemach informatycznych*, w, 2001, PWN

Literatura uzupełniająca

[1] Aeleen Frisch — *Unix. Administracja systemu.*, Warszawa, 2003, Wydawnictwo RM

[2] Cheswick W. — *Firewalle i bezpieczeństwo w sieci*, Warszawa, 2003, Helion

Literatura dodatkowa

[1] Dokumentacja techniczna systemów operacyjnych i urządzeń sieciowych (Manual, White Papers)

12 Informacje o nauczycielach akademickich

Osoba odpowiedzialna za kartę

dr inż. Paweł, Marek Brandys (kontakt: `brandys@mech.pk.edu.pl`)

Osoby prowadzące przedmiot

1 dr inż. Paweł Brandys (kontakt: `brandys@mech.pk.edu.pl`)

2 mgr inż. Mariusz Krawczyk (kontakt: `Mariusz.Krawczyk@mech.pk.edu.pl`)

13 Zatwierdzenie karty przedmiotu do realizacji

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

Przyjmuję do realizacji (data i podpisy osób prowadzących przedmiot)

. . . . . .

. . . . . .