

POLITECHNIKA KRAKOWSKA IM. TADEUSZA KOŚCIUSZKI

KARTA PRZEDMIOTU

obowiązuje studentów rozpoczynających studia w roku akademickim 2013/2014

Wydział Fizyki, Matematyki i Informatyki

Kierunek studiów: Informatyka

Profil: Ogólnoakademicki

Forma studiów: 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 13/14 |
| KATEGORIA PRZEDMIOTU | Przedmioty specjalnościowe |
| LICZBA PUNKTÓW ECTS | 5.00 |
| SEMESTRY | 6 |

2 RODZAJ ZAJĘĆ, LICZBA GODZIN W PLANIE STUDIÓW

| SEMESTR | WYKŁAD | ĆWICZENIA | LABORATORIUM | LABORATORIUM KOMPUTERO- WE | 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

| LABORATORIUM | | |
|--------------|--|------------------|
| LP | TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH | LICZBA GODZIN |
| L1 | Omówienie zasad, prezentacja sprzętu, zapoznanie z wykorzystywanym oprogramowaniem | 2 |
| L2 | Quick Setup Wizard, zapoznanie z WSM i FSM | 2 |
| L3 | Tworzenie polityk, logi | 2 |
| L4 | Tworzenie polityk proxy | 2 |
| L5 | Serwer zarządzania, serwer raportów, serwer kwarantanny, serwer WebBlocker | 2 |
| L6 | Autentykacja użytkowników | 2 |
| L7 | MOVPN z PPTP | 2 |
| L8 | MOVPN z IPsec | 2 |
| L9 | MOVPN z SSL | 2 |
| L10 | BOVPN | 2 |

| LABORATORIUM | | |
|--------------|---|------------------|
| LP | TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH | LICZBA GODZIN |
| L11 | MultiWAN | 2 |
| L12 | WebBlocker, AV/IPS, spamBlocker, RED, application control | 2 |
| L13 | Troubleshooting | 6 |

| WYKŁAD | | |
|------------|--|------------------|
| LP | TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH | LICZBA GODZIN |
| W1 | Wstęp, omówienie zasad zaliczenia, omówienie podstawowych pojęć związanych z bezpieczeństwem | 2 |
| W2 | Podstawy kryptografii | 4 |
| W3 | Podpis cyfrowy, PKI, standard X.509 | 2 |
| W4 | Bezpieczeństwo sieci komputerowych, omówienie zagrożeń poszczególnych warstw modelu OSI, przedstawienie koncepcji różnego rodzaju technik ataków | 6 |
| W5 | Prezentacja w rzeczywistym systemie zagrożeń bezpieczeństwa, technik ataków i obrony | 4 |
| W6 | Firewall, VPN, PGP | 2 |
| W7 | IPSec, IKE, Kerberos | 2 |
| W8 | Protokół IPSec. | 2 |
| W9 | Bezpieczeństwo sieci bezprzewodowych | 2 |
| W10 | Bezpieczeństwo systemów | 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 | 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 SZCZEGÓLOWYCH 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 | L1 L2 L3 L4 L5 L6 L7 L8 L9 L10 L11 L12 L13 W1 | 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 | N1 N2 N3 N4 | F2 P1 P2 |
| EK4 | I1_W14 | Cel 1 | W2 W3 W7 | 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] Eric Cole, Ronald L. Krutz, James Conley — *Bezpieczeństwo sieci: biblia.*, Gliwice, 2005, Helion
- [3] Libor Dostalek — *Bezpieczeństwo protokołu TCP/IP: kompletny przewodnik.*, Warszawa, 2006, PWN
- [4] William Stallings — *Kryptografia i bezpieczeństwo sieci komputerowych: koncepcje i metody bezpiecznej komunikacji.*, Gliwice, 2012, Helion
- [5] Marek Serafin — *Sieci VPN: zdalna praca i bezpieczeństwo danych.*, Gliwice, 2010, Helion

12 INFORMACJE O NAUCZYCIELACH AKADEMICKICH

OSOBA ODPOWIEDZIALNA ZA KARTĘ

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

OSOBY PROWADZĄCE PRZEDMIOT

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

2 mgr inż. Michał Niedźwiecki (kontakt: nkg753@gmail.com)

13 ZATWIERDZENIE KARTY PRZEDMIOTU DO REALIZACJI

(miejsowość, data)

(odpowiedzialny za przedmiot)

(dziekan)

PRZYJMUJĘ DO REALIZACJI (data i podpisy osób prowadzących przedmiot)

.....

.....