

# POLITECHNIKA KRAKOWSKA IM. TADEUSZA KOŚCIUSZKI

## KARTA PRZEDMIOTU

obowiązuje studentów rozpoczynających studia w roku akademickim 2014/2015

Wydział Fizyki, Matematyki i Informatyki

Kierunek studiów: Informatyka

Profil: Ogólnoakademicki

Forma studiów: niestacjonarne

Kod kierunku: I

Stopień studiów: II

Specjalności: Teleinformatyka dla licencjatów

### 1 INFORMACJE O PRZEDMIOCIE

|                                         |                                             |
|-----------------------------------------|---------------------------------------------|
| NAZWA PRZEDMIOTU                        | Bezpieczeństwo systemów teleinformatycznych |
| NAZWA PRZEDMIOTU<br>W JĘZYKU ANGIELSKIM |                                             |
| KOD PRZEDMIOTU                          | WFMiI I oIIN D8 14/15                       |
| KATEGORIA PRZEDMIOTU                    | Przedmioty specjalnościowe                  |
| LICZBA PUNKTÓW ECTS                     | 4.00                                        |
| SEMESTRY                                | 4                                           |

### 2 RODZAJ ZAJĘĆ, LICZBA GODZIN W PLANIE STUDIÓW

| SEMESTR | WYKŁAD | ĆWICZENIA | LABORATORIUM | LABORATORIUM<br>KOMPUTERO-<br>WE | SEMINARIUM | PROJEKT |
|---------|--------|-----------|--------------|----------------------------------|------------|---------|
| 4       | 18     | 0         | 18           | 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 sprzętowymi, 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 Umiejętności** Student potrafi konfigurować zaawansowane funkcjonalności bezpieczeństwa dla urządzeń klasy XTM.

**EK2 Umiejętności** Student potrafi konfigurować urządzenia klasy SSL VPN Gateway.

**EK3 Wiedza** Student potrafi przedstawić i omówić zasadę działania podstawowych protokołów sieciowych gwarantujących bezpieczeństwo transmisji danych w sieciach teleinformatycznych.

**EK4 Wiedza** Student potrafi przedstawić i omówić podstawowe techniki przeprowadzania testów zabezpieczeń systemów teleinformatycznych.

## 6 TREŚCI PROGRAMOWE

| WYKŁAD     |                                                                                      |                  |
|------------|--------------------------------------------------------------------------------------|------------------|
| LP         | TEMATYKA ZAJĘĆ<br>OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH                               | LICZBA<br>GODZIN |
| <b>W1</b>  | Wstęp, omówienie zasad zaliczenia, prezentacja tematyki przedmiotu.                  | 2                |
| <b>W2</b>  | Prezentacja protokołu SSL.                                                           | 2                |
| <b>W3</b>  | Prezentacja usługi DNSSec.                                                           | 1                |
| <b>W4</b>  | Omówienie technik łamania haseł.                                                     | 1                |
| <b>W5</b>  | Prezentacja systemów klasy SSL VPN Gateway.                                          | 2                |
| <b>W6</b>  | Prezentacja systemów DLP.                                                            | 2                |
| <b>W7</b>  | Prezentacja systemów HoneyPot.                                                       | 2                |
| <b>W8</b>  | Prezentacja zagrożeń płynących z sieci P2P.                                          | 1                |
| <b>W9</b>  | Omówienie podstawowych technik zbierania informacji o systemach teleinformatycznych. | 1                |
| <b>W10</b> | Omówienie technik testowania zabezpieczeń systemów teleinformatycznych.              | 1                |
| <b>W11</b> | Bezpieczeństwo serwera sieciowego.                                                   | 2                |
| <b>W12</b> | Omówienie dystrybucji narzędziowej BackTrack.                                        | 1                |

| LABORATORIUM |                                                                                                                   |                  |
|--------------|-------------------------------------------------------------------------------------------------------------------|------------------|
| LP           | TEMATYKA ZAJĘĆ<br>OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH                                                            | LICZBA<br>GODZIN |
| <b>L1</b>    | Instalacja i konfiguracja systemu operacyjnego jako elementu wspierającego pracę urządzeń bezpieczeństwa.         | 1                |
| <b>L2</b>    | Konfigurowanie urządzeń klasy XTM z wykorzystaniem transparentnej autentykacji użytkowników.                      | 1                |
| <b>L3</b>    | Konfigurowanie funkcjonalności filtrowania spamu z kwarantanną dla urządzeń klasy XTM.                            | 1                |
| <b>L4</b>    | Konfigurowanie funkcjonalności IPS dla urządzeń klasy XTM.                                                        | 1                |
| <b>L5</b>    | Testowanie zabezpieczeń realizowanych przez urządzenia klasy XTM.                                                 | 1                |
| <b>L6</b>    | Zapoznanie z podstawowymi elementami konfiguracji urządzeń klasy SSL VPN Gateway.                                 | 1                |
| <b>L7</b>    | Konfiguracja poszczególnych sposobów autentykacji użytkowników w urządzeniach klasy SSL VPN Gateway.              | 2                |
| <b>L8</b>    | Integracja systemu klasy SSL VPN Gateway z Active Directory.                                                      | 1                |
| <b>L9</b>    | Tworzenie dostępnych zasobów w urządzeniach klasy SSL VPN Gateway.                                                | 2                |
| <b>L10</b>   | Weryfikacja poziomu bezpieczeństwa komputera, z którego następuje połączenie do urządzenia klasy SSL VPN Gateway. | 2                |
| <b>L11</b>   | Usuwanie danych tymczasowych na komputerze z którego nastąpiło połączenie do urządzenia klasy SSL VPN Gateway.    | 1                |
| <b>L12</b>   | Personalizacja portalu z zasobami.                                                                                | 1                |
| <b>L13</b>   | Zbieranie logów oraz generowanie raportów aktywności dla urządzeń klasy SSL VPN Gateway.                          | 1                |
| <b>L14</b>   | Sprawdzian umiejętności konfigurowania urządzeń klasy SSL VPN Gateway.                                            | 2                |

## 7 NARZĘDZIA DYDAKTYCZNE

**N1** Wykłady

**N2** Ćwiczenia laboratoryjne

**N3** Prezentacje multimedialne

**N4** Konsultacje

## 8 OBCIĄŻENIE PRACĄ STUDENTA

| FORMA AKTYWNOŚCI                                                                                 | ŚREDNIA LICZBA GODZIN<br>NA ZREALIZOWANIE<br>AKTYWNOŚCI |
|--------------------------------------------------------------------------------------------------|---------------------------------------------------------|
| <b>Godziny kontaktowe z nauczycielem akademickim, w tym:</b>                                     |                                                         |
| Godziny wynikające z planu studiów                                                               | 36                                                      |
| Konsultacje przedmiotowe                                                                         | 0                                                       |
| Egzaminy i zaliczenia w sesji                                                                    | 0                                                       |
| <b>Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:</b> |                                                         |
| Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury                               | 84                                                      |
| Opracowanie wyników                                                                              | 0                                                       |
| Przygotowanie raportu, projektu, prezentacji, dyskusji                                           | 0                                                       |
| <b>SUMARYCZNA LICZBA GODZIN DLA PRZEDMIOTU WYNIKAJĄCA Z<br/>CAŁEGO NAKŁADU PRACY STUDENTA</b>    | <b>120</b>                                              |
| 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 kolokwium 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               | I2_U06, I2_U10, I2_U11                                                         | Cel 1           | W1 W8 W11         | N1 N2 N3 N4           | F1 F2 P1 P2   |
| EK2               | I2_U06, I2_U10, I2_U11                                                         | Cel 2           | W5 W6 W7          | N1 N2 N3 N4           | F1 F2 P1 P2   |
| EK3               | I2_W03                                                                         | Cel 3           | W2 W3             | N1 N3 N4              | F2 P1 P2      |
| EK4               | I2_W02                                                                         | Cel 4           | W4 W9 W10 W11 W12 | N1 N2 N3 N4           | F1 F2 P1 P2   |

## 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 linuxowych 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

Marcin Klamra (kontakt: mklamra@15.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)

.....  
.....