**Nazwa przedmiotu:**

Bezpieczeństwo systemów i sieci

**Koordynator przedmiotu:**

Krzysztof CABAJ

**Status przedmiotu:**

Fakultatywny ograniczonego wyboru

**Poziom kształcenia:**

Studia I stopnia

**Program:**

Informatyka

**Grupa przedmiotów:**

Przedmioty techniczne

**Kod przedmiotu:**

BSS

**Semestr nominalny:**

5 / rok ak. 2014/2015

**Liczba punktów ECTS:**

4

**Liczba godzin pracy studenta związanych z osiągnięciem efektów uczenia się:**

103h (30h wykład, 15h ćwiczenia laboratoryjne, 3h egzamin, 30h przygotowanie do ćwiczeń, 25h przygotowanie do egzaminu)

**Liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich:**

2 ECTS (30h wykładu, 15h ćwiczeń, 3h egzamin)

**Język prowadzenia zajęć:**

polski

**Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym:**

2 ECTS (15h ćwiczeń, 30h przygotowania do ćwiczeń)

**Formy zajęć i ich wymiar w semestrze:**

|  |  |
| --- | --- |
| Wykład:  | 30h |
| Ćwiczenia:  | 0h |
| Laboratorium:  | 15h |
| Projekt:  | 0h |
| Lekcje komputerowe:  | 0h |

**Wymagania wstępne:**

-

**Limit liczby studentów:**

120

**Cel przedmiotu:**

Głównym celem przedmiotu jest uświadomienie słuchaczom z jakimi zagrożeniami ma do czynienia dzisiejszy użytkownik Internetu,
administrator systemów teleinformatycznych czy programista. W ramach wykładu omawiane są podstawowe oraz aktualnie najpopularniejsze
rodzaje ataków oraz różnorakie techniki i mechanizmy obrony. O ile to możliwe prezentowane zagadnienia omawiane są na rzeczywistych
przykładach złośliwego kodu, ataków czy błędów w programach lub konfiguracji oprogramowania oraz urządzeń sieciowych.

**Treści kształcenia:**

Przedmiot składa się z 15 wykładów oraz siedmiu ćwiczeń laboratoryjnych.

Tematyka wykładów:
1. Wprowadzenie
2. Szyfry symetryczne/asymetryczne
3. Funkcje skrótu - uwierzytelnienie
4. Infrastruktura klucza publicznego
5. Wprowadzenie do zagrożeń sieciowych
6. Bezpieczeństwo aplikacji C/C++
7. Wirusy, robaki, konie trojańskie (malware I)
8. Wirusy, robaki, konie trojańskie (malware II)
9. Bezpieczeństwo aplikacji Webowych
10. Karty inteligentne
11. Systemy zapewniających bezpieczeństwo w sieciach komputerowych
12. Mechanizmy bezpieczeństwa systemów operacyjnych
13. Mechanizmy monitorowania i logowania systemów operacyjnych
14. Systemy HoneyPot
15.Polityka bezpieczeństwa

Tematy ćwiczeń
1. Algorytmy szyfrowania 1
2. Algorytmy szyfrowania 2
3. PGP
4. Openssl
5. Stunnel
6. Systemy IDS
7. Bezpieczeństwo aplikacji

**Metody oceny:**

W ramach przedmiotu można uzyskać 100p (40p w ramach ćwiczeń laboratoryjnych oraz 60p podczas egzaminu).

Warunkiem zaliczenia przedmiotu jest uzyskanie co najmniej 21 punktów z laboratorium oraz 31 punktów z egzaminu.

**Egzamin:**

tak

**Literatura:**

1. Ross Anderson, "Inżyniera zabezpieczeń", Wydawnictwo Naukowo-Techniczne, (2005)
2. Willliam Stallings, Kryptografia i Bezpieczeństwo sieci komputerowych, cz I - Matematyka szyfrów i techniki kryptologii, wydanie V, Wydawnictwo Helion, (2012)
3. Willliam Stallings, Kryptografia i Bezpieczeństwo sieci komputerowych, cz II - Koncepcje i metody bezpiecznej komunikacji, wydanie V, Helion, (2012)
4. Bruce Schneier, "Kryptografia dla praktyków. Protokoły, algorytmy i programy źródłowe w języku C". J. Willey WNT, Warszawa, (2002)
5. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Kryptografia stosowana", Wydawnictwo Naukowo-Techniczne, (2005)
6. Simon Singh, Księga szyfrów, Wydawnictwo Świat Książki, (2003)

**Witryna www przedmiotu:**

https://studia.elka.pw.edu.pl/priv/14Z/BSS.A/

**Uwagi:**

## Efekty przedmiotowe

### Profil ogólnoakademicki - wiedza

**Efekt BSS\_W01:**

Student potrafi omówić sposób działania algorytmów szyfrowania i usługi ochrony informacji, które można zrealizować za ich pomocą.

Weryfikacja:

egzamin, ćwiczenia

**Powiązane efekty kierunkowe:** K\_W01, K\_W18

**Powiązane efekty obszarowe:** T1A\_W01, T1A\_W02, T1A\_W03, T1A\_W07, T1A\_W07, T1A\_W08

**Efekt BSS\_W02:**

Student potrafi opisać podstawowe zagrożenia dla bezpieczeństwa komputerów i sieci komputerowych oraz scharakteryzować możliwe metody obrony.

Weryfikacja:

egzamin, ćwiczenia

**Powiązane efekty kierunkowe:** K\_W18

**Powiązane efekty obszarowe:** T1A\_W07, T1A\_W08

### Profil ogólnoakademicki - umiejętności

**Efekt BSS\_U01:**

Student umie wykorzystać narzędzia bezpieczeństwa w celu zlokalizowanie podatności oraz skonfigurować odpowiedni mechanizmy je niwelujące.

Weryfikacja:

ćwiczenia

**Powiązane efekty kierunkowe:** K\_U11, K\_U20, K\_U24

**Powiązane efekty obszarowe:** T1A\_U11, T1A\_U13, T1A\_U15, T1A\_U10, T1A\_U13, T1A\_U14, T1A\_U16

**Efekt BSS\_U02:**

Umie zlokalizować w kodzie podatne konstrukcje, poprawić je lub zastosować inne rozwiązanie niwelujące dane zagrożenie.

Weryfikacja:

ćwiczenia

**Powiązane efekty kierunkowe:** K\_U02, K\_U11

**Powiązane efekty obszarowe:** T1A\_U08, T1A\_U09, T1A\_U11

### Profil ogólnoakademicki - kompetencje społeczne

**Efekt BSS\_K01:**

Student umie omówić wpływ błędów w programach i konfiguracji na bezpieczeństwo całego systemu.

Weryfikacja:

egzamin, ćwiczenia

**Powiązane efekty kierunkowe:** K\_K02

**Powiązane efekty obszarowe:** T1A\_K02

**Efekt BSS\_K02:**

Student umie realizować powierzone zadania związane z analizą zagrożeń i ich niwelacją w grupie.

Weryfikacja:

ćwiczenia

**Powiązane efekty kierunkowe:** K\_K03

**Powiązane efekty obszarowe:** T1A\_K03