**Nazwa przedmiotu:**

Bezpieczeństwo systemów i sieci

**Koordynator przedmiotu:**

Rajmund Kożuszek

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia I stopnia

**Program:**

Informatyka

**Grupa przedmiotów:**

Przedmioty techniczne

**Kod przedmiotu:**

BSS

**Semestr nominalny:**

4 / rok ak. 2021/2022

**Liczba punktów ECTS:**

4

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

1. liczba godzin kontaktowych – 55 godz., w tym
 obecność na wykładach: 30 godz.,
 obecność na zajęciach laboratoryjnych:15 godz.,
 udział w konsultacjach związanych z problematyką poruszaną na wykładzie/laboratorium: 4 godz.,
 udział w konsultacjach przedegzaminacyjnych: 4 godz.,
 obecność na egzaminie: 2 godz.

2. praca własna studenta – 55 godz., w tym
 przygotowanie do laboratoriów 25 godz.,
 analiza literatury i materiałów wykładowych związana z przygotowaniem do kolejnych wykładów: 15 godz.,
 przygotowanie do egzaminu: 15 godz.

Łączny nakład pracy studenta wynosi 110 godz., co odpowiada 4 pkt. ECTS.

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

2 pkt. ECTS, co odpowiada 55 godz. kontaktowym

**Język prowadzenia zajęć:**

polski

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

2 pkt. ECTS, co odpowiada 48 godz. zajęć laboratoryjnych oraz przygotowaniu do tych zajęć

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

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

**Wymagania wstępne:**

Systemy Operacyjne (SOI), Architektura Komputerów(ARKO), Sieci Komputerowe (SKM)

**Limit liczby studentów:**

150

**Cel przedmiotu:**

Głównym celem przedmiotu jest uświadomienie słuchaczom, z jakimi zagrożeniami ma do czynienia dzisiejszy użytkownik Internetu, administrator systemów teleinformatycznych oraz programista. W ramach wykładu omawiane są podstawowe oraz aktualnie najpopularniejsze rodzaje ataków oraz różnorakie techniki i mechanizmy obrony. Omówieniu poddane są wykorzystywane przez nie podatności i błędy w oprogramowaniu oraz konfiguracji systemów informatycznych, a także elementy socjotechniki wykorzystywane do przechwytywania wrażliwych danych Prezentowane zagadnienia omawiane są na rzeczywistych przykładach złośliwego kodu, ataków czy błędów w programach lub konfiguracji oprogramowania oraz urządzeń sieciowych.

W ramach laboratorium, studenci zapoznają się z praktycznymi aspektami konfiguracji mechanizmów bezpieczeństwa. Dodatkowo dokładnie przeanalizują błędy dydaktycznych aplikacji, które mogą prowadzić do udanego przejęcia kontroli nad systemem.

**Treści kształcenia:**

WYKŁADY:

1. Wprowadzenie do usług ochrony informacji i elementów kryptografii (szyfry symetryczne i asymetryczne, funkcja skrótu) (6 godz.),
2. Infrastruktura klucza publicznego (2 godz.),
3. Elementy bezpieczeństwa we współczesnych systemach operacyjnych (2 godz.),
4. Omówienie najpopularniejszych ataków sieciowych (2 godz.),
5. Błędy typu przepełnienie bufora (ang. buffer overflow), omówienie oraz mechanizmy (2 godz.),
6. Bezpieczeństwo serwisów WWW (2 godz.),
7. Omówienie mechanizmów bezpieczeństwa sieci komputerowych: zapory ogniowe, systemy IDS, systemy SIEM, mechanizmy obrony w warstwie drugiej modelu ISO/OSI (2 godz.),
8. Mechanizmy logowania i monitorowania - wykorzystanie w bezpieczeństwie (2 godz.),
9. Złośliwe oprogramowanie, sposób działania, ewolucja na przestrzeni ostatnich kilku lat (5 godz.),
10. Systemy HoneyPot (2 godz.),
11. Omówienie elementów socjotechniki w atakach (1 godz),
12. Polityka bezpieczeństwa, szacowanie ryzyka (2 godz.).

LABORATORIUM:

W ramach laboratoriów studenci praktycznie zapoznają się z omawianymi na wykładzie zagadnieniami podczas ich konfiguracji. Ocena wystawiana jest podstawie pokazu działania wskazanych przez prowadzącego skonfigurowanych funkcji lub na podstawie sprawozdania.

1. Uruchomienie CA, wystawiania certyfikatów,
2. Korzystanie z szyfrowanej poczty,
3. Konfiguracja zapory ogniowej,
4. Konfiguracja tunelu VPN - OpenSSL lub IPSec,
5. Uruchomienie systemu IDS - Snort,
6. Analiza błędów w serwisach WWW,
7. Atak na aplikację podatną na przepełnienia bufora.

**Metody oceny:**

Realizacja przedmiotu obejmuje następujące formy zajęć:
 wykład prowadzony w wymiarze 2 godz. tygodniowo;
 zajęcia laboratoryjne (7 dwugodzinnych zajęć w semestrze); w ramach tych zajęć, student, korzystając z oprogramowania i sprzętu, będzie – pod opieką prowadzącego zajęcia – realizował wskazane zadania związane tematycznie z treścią wykładu.

Sprawdzanie założonych efektów kształcenia realizowane jest przez:
 ocenę wiedzy i umiejętności związanych z realizacją zadań laboratoryjnych – ocenę sprawozdań z realizacji zadań;
 ocenę wiedzy i umiejętności wykazanych na egzaminie pisemnym o charakterze problemowym.

**Egzamin:**

tak

**Literatura:**

Witryny internetowe:
Internet Storm Center, Handler Diary, https://dshield.org/
Niebezpiecznik, https://niebezpiecznik.pl/
Zaufana Trzecia Strona, https://zaufanatrzeciastrona.pl/

Książki:
- Ross Anderson, "Inżyniera zabezpieczeń", Wydawnictwo Naukowo-Techniczne, (2005)
- Bruce Schneier, "Kryptografia dla praktyków. Protokoły, algorytmy i programy źródłowe w języku C". J. Willey WNT, Warszawa, (2002)
- Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Kryptografia stosowana", Wydawnictwo Naukowo-Techniczne, (2005)

**Witryna www przedmiotu:**

https://usosweb.usos.pw.edu.pl/kontroler.php?\_action=katalog2/przedmioty/pokazPrzedmiot&prz\_kod=103B-INxxx-ISP-BSS

**Uwagi:**

(-)

## Charakterystyki przedmiotowe

### Profil ogólnoakademicki - wiedza

**Charakterystyka W01:**

zna sposób działania algorytmów szyfrowania oraz usługi ochrony informacji, które można zrealizować za ich pomocą

Weryfikacja:

laboratorium, egzamin

**Powiązane charakterystyki kierunkowe:** W01

**Powiązane charakterystyki obszarowe:** P6U\_W, I.P6S\_WG.o

**Charakterystyka W02:**

zna podstawowe zagrożenia dla bezpieczeństwa komputerów i sieci komputerowych oraz możliwe metody obrony

Weryfikacja:

laboratorium, egzamin

**Powiązane charakterystyki kierunkowe:** W10

**Powiązane charakterystyki obszarowe:** P6U\_W, I.P6S\_WG.o, III.P6S\_WG

### Profil ogólnoakademicki - umiejętności

**Charakterystyka U01:**

umie wykorzystać narzędzia bezpieczeństwa w celu zlokalizowania podatności na atak

Weryfikacja:

laboratorium

**Powiązane charakterystyki kierunkowe:** U01

**Powiązane charakterystyki obszarowe:** P6U\_U, I.P6S\_UW.o, III.P6S\_UW.o

**Charakterystyka U02:**

umie zlokalizować w kodzie programu podatne na atal konstrukcje, poprawić je lub zastosować inne rozwiązanie niwelujące dane zagrożenie

Weryfikacja:

laboratorium

**Powiązane charakterystyki kierunkowe:** U05, U06

**Powiązane charakterystyki obszarowe:** I.P6S\_UW.o, III.P6S\_UW.o, P6U\_U

**Charakterystyka U03:**

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

Weryfikacja:

laboratorium

**Powiązane charakterystyki kierunkowe:** U08

**Powiązane charakterystyki obszarowe:** P6U\_U, I.P6S\_UO

**Charakterystyka U04:**

potrafi skonfigurować odpowiednie mechanizmy bezpieczeństwa bazując na dostarczonej dokumentacji w języku angielskim

Weryfikacja:

laboratorium

**Powiązane charakterystyki kierunkowe:** U11

**Powiązane charakterystyki obszarowe:** P6U\_U, I.P6S\_UK

### Profil ogólnoakademicki - kompetencje społeczne

**Charakterystyka K01:**

jest gotów do ciągłego poznawania nowych metod ataku oraz sposobów przeciwdziałania

Weryfikacja:

laboratorium

**Powiązane charakterystyki kierunkowe:** K01

**Powiązane charakterystyki obszarowe:** P6U\_K, I.P6S\_KK

**Charakterystyka K02:**

jest świadomy metod socjotechnicznych stanowiących zagrożenie dla bezpieczeństwa wrażliwych systemów informatycznych

Weryfikacja:

egzamin

**Powiązane charakterystyki kierunkowe:** K02

**Powiązane charakterystyki obszarowe:** P6U\_K, I.P6S\_KR