KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Bezpieczeństwo w sieciach bezprzewodowych

Przedmiot

Kierunek studiów

Elektronika i Telekomunikacja

Rok/semestr

1/2

Studia w zakresie (specjalność)

Sieci komputerowe i technologie internetowe

Profil studiów

ogólnoakademicki

Poziom studiów

drugiego stopnia

Język oferowanego przedmiotu

polski

Forma studiów

stacjonarne

Wymagalność

obieralny

Liczba godzin

Wykład

30

Laboratoria

15

Inne (np. online)

Ćwiczenia

15

Projekty/seminaria

Liczba punktów ECTS

4

Wykładowcy

Odpowiedzialny za przedmiot/wykładowca:

dr inż. Sławomir Hanczewski,
slawomir.hanczewski@put.poznan.pl

Odpowiedzialny za przedmiot/wykładowca:

Wymagania wstępne

Student rozpoczynający ten przedmiot powinien posiadać uporządkowaną wiedzę z zakresu budowy i działania sieci komputerowych (w tym sieci bezprzewodowych) obejmującą zarówno urządzania, jaki i protokoły sieciowe. Powinien również rozumieć konieczność poszerzania swoich kompetencji oraz posiadać umiejętność pozyskiwania informacji ze wskazanych źródeł.

Cel przedmiotu

Przekazanie studentom teoretycznych i praktycznych zagadnień związanych z budowaniem bezpiecznych sieci bezprzewodowych i ich testowaniem oraz z świadomym i bezpiecznym korzystaniem z zasobów Internetu.

Przedmiotowe efekty uczenia się

Wiedza

Student posiada usystematyzowaną wiedzę z zakresu bezpieczeństwa sieci komputerowych obejmującą:
1. zasady działania rozwiązań zapewniających bezpieczeństwo sieci bezprzewodowych (zapory sieciowe, IPS/IDS),

2. budowę i działania wirtualnych sieci bezprzewodowych,

3. mechanizmów kryptograficznych wykorzystywanych we współczesnych sieciach.

4. testy bezpiczesńtwa.

Umiejętności

1. Potrafi konfigurować urządzenia sieciowe i oprogramowanie w sposób zapewniający bezpieczene przsyłanie danych.

2. Potrafi wykorzystać mechanizmy kryptograficzne do bezpieczenego przesyłania danych.

3. Potrafi zaplanować i przeprowadzić proste testy sieci bezprzewodowych.

4. Potrafi świadomie korzystać z zasobów Internetu.

Kompetencje społeczne

1. Jest świadomy zmian jakie zachodzą wraz z ewolucjąsieci komputerowych Zna ograniczenia własnej wiedzy i rozumie konieczność ciągłego jej uaktualniania. Jest otwarty na możliwości ciągłego dokształcania się.

2. Profesjonalnie podchodzi do rozwiązywania problemów związanych z bezpieczeństwem sieci bezprzewodowych.

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wiedza zdobyta w trakcie wykładów jest weryfikowana przez kolokwium realizowane na ostatnim wykładzie. Kolokwium składa się z 30 pytań testowych, w któych proponowane są 4 odpowiedzi, przy czym tylko jedna odpowiedź jest porawna. Próg zaliczeniowy wynosi 50%. Zagadnienia zaliczeniowe, na podstawie których opracowywane są pytania zostaną przesłane studentom drogą mailową z wykorzystaniem systemu uczelnianej poczty elektronicznej.

Wiedza zdobyta w trakcie ćwiczeń jest weryfikowana przez kolokwium realizowane na ostatnich zajęciach. Kolokwium składa się z 4 pytań otwartych, różnie punktowanych w zależności od ich trudności. Próg zaliczeniowy wynosi 50%. Zagadnienia, na podstawie których opracowywane są pytania odpowiadają treściom programowym realizowanym na ćwiczeniach.

Wiedza i umiejętności zbobyte w trakcie ćwiczeń laboratoryjnych weryfikowane jest poprzez kontrolę poprawności wykonania ćwiczenia np. kontrolując poprawność skonfigurowania urządzeń sieciowych oraz zadawanie pytań dotyczących realizowanego ćwiczenia. Brak zaliczenia ćwiczenia skutkuje koniecznością jego powtórzenia w terminie wskazanym przez prowadzącego.

Treści programowe

Wykłady:

1. Sieci komputerowe - analiza zagrożeń

2. Bezpieczeństwo urządzeń sieciowych

3. Dostęp do sieci bezprzewodowych

4. Systemy wykrywania intruzów w sieciach bezprzewodowych

5. Wardriving

6. Wirtualne Sieci Prywatne - VPN (Virtual Private Network)

7. Kryptografia

8. Testy bezpieczeństwa

Ćwiczenia

1. Analiza zagrożeń czyhających na użytkowników Internetu.

2. Analiza mechanizmów kryptograficznych zapewniających bezpieczne przesyłanie danych.

3. Analiza protokołów sieciowych zapeniających bezpieczne przesyłanie danych.

Ćwiczenia laboratoryjne:

1. Budowa sieci wykorzystujących rozwiązania bezprzewodowe.

2. Analiza możliwości łamania zabezpieczeń w sieciach bezprzewodowych.

3. Konfiguracja sprzetowego systemu wykrywania intruzów (IDS).

4. Tworzenie i konfiguracja wirtualnych sieci WLAN.

5. Przeprowadzenie prostych testów bezpieczeństwa sieci bezprzewodowych z wykorzystaniem Kali Linux.

Metody dydaktyczne

Wykład: prezentacja multimedialna uzupełniana przykładami i dodatkowymi wyjaśnieniami na tablicy. Wykłady są prowadzone z godnie z zasadami wykładu tradycyjnego, w uzasadnionych przypadkach przybierającego formę wykładu konwersatoryjnego.

Ćwiczenia: prezentacja multimedialna, ćwiczenia tablicowe obejmujące omawiane algorytmy kryptograficzne oraz protokoły sieciowe.

Ćwiczenia laboratoryjne: prezentacja multimedialna prezentacja ilustrowana przykładami podawanymi na tablicy oraz wykonanie zadań podanych przez prowadzącego - ćwiczenia praktyczne.

Literatura

Podstawowa

1. Ramachandran V., Buchanan C., Kali Linux : audyt bezpieczeństwa sieci Wi-Fi dla każdego, Helion 2016

2. Kim P., Podręcznik pentestera : bezpieczeństwo systemów informatycznych, Helion 2015.

3. Stallings W., Kryptografia i bezpieczeństwo sieci komputerowych : matematyka szyfrów i techniki kryptologii, Helion 2012].

Uzupełniająca

1. Erickson J., Hacking, Sztuka penetracji, Helion 2004

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	100	4,0
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	70	3,0
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych oraz ćwiczeń, przygotowanie do kolokwium)[1]	30	1

[1] niepotrzebne skreślić lub dopisać inne czynności