Nazwa przedmiotu							
Diagnostyka zabezpieczeń sieci Network security diagnostics							
Dyscyplina							Oznaczenie przedmiotu
Informatyka							8S_IS1
Rodzaj przedmiotu	Stopień studiów	Tryb studiów		Język zajęć		Rok	Semestr
Do wyboru	1	stacjonarne		polski		III	VI
Rodzaj zajęć		Wyk.	Ćw.	Lab.	Sem.	Proj.	Liczba punktów ECTS
Liczba godzin w semestrze		15	0	15	0	0	2 ECTS
Koordynator	dr inż. Łukasz Piątek l_piatek@el.pcz.czest.pl						
Prowadzący	dr inż. Łukasz Piątek l_piatek@el.pcz.czest.pl dr inż. Piotr Szeląg szelag@el.pcz.czest.pl mgr inż. Marcjan Nowak m.nowak@el.pcz.czest.pl						

I. KARTA PRZEDMIOTU

Cel przedmiotu

C1. Zapoznanie się z zabezpieczeniami sieci komputerowych
C2. Zapoznanie się z narzędziami oraz metodami obrony sieci przed atakami na sieci przewodowe i bezprzewodowe
C3. Nauka wykrywania naruszenia zabezpieczeń sieci z wykorzystaniem specjalistycznego oprogramowania

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1. Znajomość metod zabezpieczenia sieci komputerowej przed nieautoryzowanym dostępem
2. Umiejętność konfiguracji zapory sieciowej
3. Umiejętność posługiwania się skanerami sieciowymi oraz pisania prostych programów analizujących sieć.

Efekty kształcenia

EK1. Student potrafi skutecznie zabezpieczyć sieć przed nieautoryzowanym dostępem.
EK2. Student potrafi uruchomić oraz odpowiednio skonfigurować zaporę sieciową.
EK3. Student zna najnowsze metody obrony sieci przed atakami zewnętrznymi.

Treści programowe: wykłady	Liczba godzin
W1 – Wstęp do diagnostyki zabezpieczeń sieci	1
W2-3 – Podstawowa konfiguracja zabezpieczeń sieci dla systemu Windows	2
W4-5 – Podstawowa konfiguracja zabezpieczeń sieci dla systemu Unix	2
W6 – Ochrona przed analizą ruchu sieciowego	1
W7 – Tunelowanie SSH z wykorzystaniem specjalistycznego oprogramowania	1
W8 – Ochrona przed wyłudzaniem danych	1
W9-10 – Szyfrowanie poczty i plików	2
W11-12 – Zapory sieciowe	2
W13 – Szyfrowanie i zabezpieczanie usług	1
W14 – Bezpieczeństwo sieci bezprzewodowych	1
W15 – Wykrywanie włamań do sieci	1
SUMA	**15**

Treści programowe: laboratorium	Liczba godzin
L1– Konfiguracja zapory sieciowej dla systemu Windows	1
L2-3 – Zabezpieczenie punktów montowania oraz konfiguracja usługi haseł jednorazowych dla systemów Unixowych	2
L4-5 – Wykorzystanie metody trasowania cebulowego do ochrony przed analizą ruchu sieciowego	2
L6 – Konfiguracja tunelu SSH	1
L7 – Konfiguracja narzędzi do ochrony przed wyłudzeniem danych	1
L8-9 – Zabezpieczenie serwera poczty z wykorzystaniem TLS	2
L10 - Zabezpieczenie bazy MySQL w środowisku Debian	1
L11-12 – Konfiguracja mechanizmów zabezpieczających przed identyfikacją systemu operacyjnego	2
L13 – Konfiguracja zabezpieczeń sieci bezprzewodowych	1
L14-15 – Uruchomienie oraz konfiguracja narzędzi do wykrywania włamań do sieci	2
SUMA	**15**

Narzędzia dydaktyczne
1. Prezentacja multimedialna (wykład)
2. Oprogramowanie - Linux Debian, Windows Serwer, Visual Studio

Sposoby oceny efektów kształcenia (F – ocena Formująca, P – ocena Podsumowująca)
F1. Aktywność na wykładach (dyskusja)
P1. Kolokwium / test

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z prowadzącym	30
Zapoznanie się ze wskazaną literaturą	5
Przygotowanie do zajęć	15
Przygotowanie do testu / kolokwium / egzaminu	5
Przygotowanie sprawozdań/prezentacji	5
Sumaryczna liczba godzin/punktów ECTS dla przedmiotu	**60/2 ECTS**

Wykaz literatury podstawowej i uzupełniającej

1. Lockhart A. *125 sposobów na bezpieczeństwo sieci. Wydanie II,* Wydawnictwo HELION, 2007 r.
2. Farbaniec D. *Cyberwojna. Metody działania hakerów,* Wydawnictwo HELION, 2018 r.
3. Chris Fry, Martin Nystrom.*: Monitoring i bezpieczeństwo sieci*, O'Reilly, Gliwice 2011

Macierz realizacji efektów kształcenia

Efekt kształcenia	Odniesienie efektu do efektów kształcenia dla dyscypliny naukowej Informatyka	Cele przedmiotu	Forma zajęć	Narzędzia dydaktyczne	Sposób oceny
EK1	KINF1_W06	C1	W, Lab	1,2	F1, P1
EK2	KINF1_W06	C2	W, Lab	1,2	F1, P1
EK3	KINF1_W06	C3	W, Lab	1,2	F1, P1

* – wg załącznika

II. FORMY OCENY – SZCZEGÓŁY

Ocena	Efekty
EK1	**Student potrafi skutecznie zabezpieczyć sieć przed nieautoryzowanym dostępem.**
2	Student nie zna żadnej metody zabezpieczania sieci
3	Student zna i potrafi scharakteryzować przynajmniej jedną metodę zabezpieczania sieci
3.5	Student zna i potrafi scharakteryzować przynajmniej dwie metody zabezpieczania sieci
4	Student zna i potrafi scharakteryzować przynajmniej trzy metody zabezpieczania sieci
4.5	Student zna i potrafi scharakteryzować przynajmniej cztery metody zabezpieczania sieci
5	Student zna i potrafi scharakteryzować przynajmniej pięć metod zabezpieczania sieci
EK2	**Student potrafi uruchomić i skonfigurować zaporę sieciową**
2	Student nie potrafi uruchomić lub skonfigurować zapory sieciowej
3	Student potrafi uruchomić zaporę sieciową korzystając z domyślnej konfiguracji
3.5	Student potrafi uruchomić zaporę sieciową oraz scharakteryzować wybrany jeden parametr konfiguracji
4	Student potrafi uruchomić zaporę sieciową oraz scharakteryzować wybrane dwa parametry konfiguracji
4.5	Student potrafi uruchomić zaporę sieciową oraz scharakteryzować wybrane cztery parametry konfiguracji
5	Student potrafi uruchomić zaporę sieciową oraz scharakteryzować wybrane pięć parametrów konfiguracji
EK3	**Student zna metody ataku na sieć**
2	Student nie zna metod ataku na sieć
3	Student zna i potrafi scharakteryzować przynajmniej jedną metodę ataku na sieć
3.5	Student zna i potrafi scharakteryzować przynajmniej dwie metody ataku na sieć
4	Student zna i potrafi scharakteryzować przynajmniej trzy metody ataku na sieć
4.5	Student zna i potrafi scharakteryzować przynajmniej cztery metody ataku na sieć
5	Student zna i potrafi scharakteryzować przynajmniej pięć metod ataku na sieć

III. INNE PRZYDATNE INFORMACJE O PRZEDMIOCIE

1. Wszelkie informacje dla studentów na temat planu zajęć dostępne są na tablicy ogłoszeń oraz na stronie el.pcz.pl.
2. Informacje na temat warunków zaliczania zajęć przekazywana jest studentom podczas pierwszych zajęć.