KARTA PRZEDMIOTU

Nazwa przedmiotu: ***Bezpieczeństwo sieci i systemów (TIAu>SI6-BSiS-19)***
Nazwa w języku polskim:
Nazwa w jęz. angielskim: ***Security of networks and systems***

Dane dotyczące przedmiotu:

Jednostka oferująca przedmiot: Wydział Automatyki, Elektroniki i Informatyki
Przedmiot dla jednostki: Politechnika Śląska

Domyślny typ protokołu dla przedmiotu:

EGZ

Język wykładowy:

polski

Strona WWW:

https://platforma2.polsl.pl/rau2/course/view.php?id=648

Skrócony opis:

Celem przedmiotu jest przedstawienie zagadnień związanych z bezpieczeństwem sieci i systemów komputerowych. Studenci zapoznają się z metodami oceny stanu bezpieczeństwa systemów sieciowych, technikami wykrywania i monitorowania ataków oraz technicznymi i nie-technicznymi środkami ochrony przed zagrożeniami.

Opis:

Treści programowe:

Wykład:
Model klasyczny bezpieczeństwa, klasyfikacja systemów, klasyfikacja zagrożeń, kryteria bezpieczeństwa, analiza ryzyka, zasady doboru metod zapobiegania zagrożeniom.
Zarządzanie bezpieczeństwem, zasady tworzenia polityk bezpieczeństwa, przykłady polityk.
Modele zagrożeń dla systemów IT - ataki zewnętrzne, programy autonomiczne (wormy internetowe, mailowe, wirusy, konie trojańskie), ataki skryptowe, włamania celowane, ataki socjotechniczne.
Metody wykrywania zagrożeń - analiza logów, audyt komunikacji sieciowej, analiza śladów w systemach (network, system forensic), systemy IDS, IPS.
Zmiany modelu bezpieczeństwa - zanik granic fizycznych środowiska sieci, dostępność urządzeń mobilnych z komunikacją bezprzewodową, model zdalnej pracy, BYOD.
Nowe modele działania zagrożeń - mechanizmy polimorfizmu, metamorfizmu, ukrywania programów w systemie, roboty programowe (boty), sieci botnet, rozwój biznesowego wykorzystywania zainfekowanych komputerów.
Zmiany metod ochrony - system osobną twierdzą, z wielopoziomową ochroną, technologie monitorowania komunikacji sieciowej (audyt transakcji sieciowych, analiza przepływów w sieci, metody wizualizacji aktywności sieciowej systemów, analiza relacji komunikacyjnych w sieci), monitorowanie obecności zagrożeń w sieci (systemy honeypot)

Laboratorium:
Celem laboratorium jest zapoznanie studentów z przykładowymi rozwiązaniami systemów monitorowania zagrożeń, metodami ich konfiguracji i sposobami analizowania rezultatów ich działania. Ćwiczenia prowadzone są na maszynach wirtualnych na wydzielonej sieci.
1. System Host_IDS - monitorowanie integralności systemu plików.
2. Badanie systemu wykrywania zagrożeń sieciowych (Net_IDS).
3. Narzędzia monitorowania konfiguracji bezpieczeństwa systemu.
4. Monitorowanie przebiegu infekcji malware - system honeypot.
5. Testowanie stanu bezpieczeństwa systemu - testy penetracyjne.
6. Konfiguracja systemów ochrony przed zagrożeniami.

Liczba punktów ECTS: 5
Całkowita liczba godzin: 125h (kontaktowo 65h / praca własna 60h)
Wykład: 30h
Laboratorium: 30h
Inne (omówienie sprawozdań): 5h

Praca własna studenta: przygotowanie do laboratoriów, sprawozdań, zapoznanie się z literaturą, przygotowanie do egzaminu

w tym
Liczba punktów ECTS uzyskanych w ramach zajęć prowadzonych z bezpośrednim udziałem nauczycieli akademickich: 2

Literatura:

William Stallings, Kryptografia i bezpieczeństwo sieci komputerowych. Koncepcje i metody bezpiecznej komunikacji, Helion 2012.
Clercq J., Grillenmeier G.: Bezpieczeństwo Microsoft Windows. Podstawy praktyczne, PWN, 2008
Liderman K.: Analiza ryzyka i ochrona informacji w systemach komputerowych, PWN 2009
Liderman K.: Bezpieczeństwo Informacyjne, PWN 2012
Metasploit Przewodnik po testach penetracyjnych, Wydawnictwo: Helion, 2013.
Mitnick K., Simon W.: Sztuka podstępu, Wydawnictwo: Helion 2003

Efekty uczenia się:

Wiedza
Student zna i rozumie:
Zasady i metody konfigurowania bezpiecznego działania systemów komputerowych w sieci, sposoby bezpiecznej wymiany informacji i korzystania z systemów w sieci (K1A_W08)
Zasady organizacji ochrony przed niepowołanym dostępem do systemów, wykrywania i eliminacji występujących zagrożeń, bezpiecznego przetwarzania i przechowywania danych (K1A_W12)

Umiejętności

Student potrafi
Wyszukać informacje zwiazane z działaniem okreslonego typu programów malware w systemie (objawy wskazujące na infekcję systemu) i sposobów zabezpieczania się przed nimi (K1A_U05)
przeprowadzić analize natężenia ruchu pakietów w sieci i okreslić warunki występowania anomalii statystycznych ruchu w komunikacji systemu (K1A_U12)
zaprojektować konfigurację wybranych systemów dzielących sieć na segmenty o różnym poziomie ochrony, skonfigurować je i przetestować ich funkcjonowanie (K1A_U21)
zaplanować i zrealizować testy monitorujące dostępność usług systemu w różnych częściach środowiska sieciowego (K1A_U26)
Przeanalizować obowiązujące polityki systemowe i ocenić ich wpływ na sposób wykonywania zadań przez pracowników w takim środowisku (K1A_U15)
Przeprowadzić analizę sposobu ochrony przed zagrożeniami systemu informatycznego i ocenić funkcjonalność danego rozwiązania (K1A_U33)..

Metody i kryteria oceniania:

Kurs BSiS składa się z dwóch części: wykładu i 6 ćwiczeń laboratoryjnych. Znajomość materiał z wykładu jest sprawdzany na pisemnym egzaminie, ocenianym w skali 0 do 100 pkt., do zaliczenia wymagane jest uzyskanie oceny OE co najmniej 50 pkt.
Sprawozdania z wykonania ćwiczeń laboratoryjnych oceniane są w podobnej skali, wymagane jest uzyskanie pozytywnych (> 50 pkt) ocen z każdego ćwiczenia, wyliczana jest z nich średnia SL
Ocena końcowa K wyliczana jest jako K = 0,7 * OE + 0,3 * SL

Sylabus obowiązuje od roku akademickiego 2024/25, a jego zawartość nie podlega zmianom w trakcie trwania semestru

Punkty przedmiotu w cyklach:

Teleinformatyka, stacjonarne I stopnia inżynierskie 7 sem. (TIAu-SI7)

Typ punktów	Liczba	Cykl pocz.	Cykl kon.
Europejski System Transferu Punktów (ECTS)	5	2020/2021-L	