Bezpieczeństwo w systemach i sieciach komputerowych - opis przedmiotu

Informacje ogólne

Nazwa przedmiotu	Bezpieczeństwo w systemach i sieciach komputerowych
Kod przedmiotu	11.3-WI-INFP-BSSK
Wydział	Wydział Informatyki, Elektrotechniki i Automatyki
Kierunek	Informatyka
Profil	ogólnoakademicki
Rodzaj studiów	pierwszego stopnia z tyt. inżyniera
Semestr rozpoczęcia	semestr zimowy 2021/2022

Informacje o przedmiocie

Semestr	5
Liczba punktów ECTS do zdobycia	5
Typ przedmiotu	obowiązkowy
Język nauczania	polski
Sylabus opracował	• dr hab. inż. Bartłomiej Sulikowski, prof. UZ

Formy zajęć

Forma zajęć	Liczba godzin w semestrze (stacjonarne)	Liczba godzin w tygodniu (stacjonarne)	Liczba godzin w semestrze (niestacjonarne)	Liczba godzin w tygodniu (niestacjonarne)	Forma zaliczenia
Wykład	30	2	18	1,2	Zaliczenie na ocenę
Laboratorium	30	2	18	1,2	Zaliczenie na ocenę

Cel przedmiotu

- wyrobienie nawyków i krytycznego spojrzenia na bezpieczeństwo systemów i sieci komputerowych

- zapoznanie z zagrożeniami i ochroną przed nimi w systemach informatycznych i sieciach komputerowych

- zapoznanie z mechanizmami zapewniania bezpieczeństwa przy realizacji transakcji internetowych

- zrozumienie istoty konieczności współpracy przy procesie zabezpieczania i monitorowania bezpieczeństwa w sieciach

- ukształtowanie podstawowych umiejętności w zakresie projektowania, uruchamiania i monitorowania systemów i sieci komputerowych

Wymagania wstępne

Sieci Komputerowe

Zakres tematyczny

Zagrożenia w sieciach teleinformatycznych. Kryteria oceny bezpieczeństwa sieci teleinformatycznej. Typy ataków na poszczególnych warstwach modelu OSI. Zabezpieczenia sprzętowe i programowe. Firewalle. Systemy wykrywania intruzów (IDS). Systemy zapobiegania zagrożeniom (IPS). Kryteria filtrowania ruchu sieciowego. Sieci VPN. Ataki DoS. Ataki MiM.

Oprogramowanie i systemy operacyjne. Zagrożenia: Wirusy, Robaki, Konie trojańskie, Spyware i inne. Ochrona: uaktualnienia systemowe, Programy antywirusowe i anty spyware. Protokoły warstwy aplikacji: SSH i SSL.

Bezpieczeństwo systemów MS Windows, Linux oraz systemów operacyjnych urządzeń mobilnych.

Stan prawny. Ustawa o ochronie informacji niejawnej i ustawa o cyberbezpieczeństwie (w zakresie odpowiednim do ochrony sieci teleinformatycznych). Certyfikacja urządzeń i systemów. Podstawy informatyki śledczej.

Kryptografia. Algorytmy symetryczne (DES, 3DES, AES, Twofish, rodzina RCx, Serpent, Mars) i asymetryczne (RSA, DH, ElGamal, ECC). Protokoły kryptograficzne. Kryptografia klucza publicznego. Jednokierunkowe funkcje skrótu. Podpis elektroniczny i jego weryfikacja. Architektura PKI. Podstawy kryptologii kwantowej.

Dostęp do systemu. Kontrola dostępu do systemu. Zarządzanie dostępem użytkowników. Zakres odpowiedzialności użytkowników. Uwierzytelnianie urządzeń i użytkowników. Architektura RADIUS i TACACS+. Mechanizmy EAP. Systemy AAA.

Bezpieczeństwo sieci bezprzewodowych. Szyfrowanie transmisji (WEP, WPA, WPA2). Bezpieczeństwo mechanizmu WPS.

Metody kształcenia

wykład: wykład konwencjonalny, dyskusja

laboratorium: ćwiczenia laboratoryjne

Efekty uczenia się i metody weryfikacji osiągania efektów uczenia się

Opis efektu	Symbole efektów	Metody weryfikacji	Forma zajęć
potrafi zdiagnozować najczęstsze typy ataków w sieciach komputerowych	• K_W18 • K_W19 • K_U14	• kolokwium	• Wykład • Laboratorium
potrafi scharakteryzować zagrożenia występujące w systemach informatycznych oraz metody ochrony przed nimi	• K_W18 • K_W19	• kolokwium	• Wykład
potrafi zaproponować i wdrożyć mechanizmy zwiększające poziom bezpieczeństwa w sieciach komputerowych	• K_W18 • K_U13 • K_U14	• kolokwium • obserwacja i ocena aktywności na zajęciach	• Wykład • Laboratorium
zna algorytmy i protokoły kryptograficzne oraz ma świadomość jak ich stosowanie zwiększa poziom bezpieczeństwa w systemach informatycznych i sieciach komputerowych	• K_W18 • K_U14	• kolokwium • obserwacja i ocena aktywności na zajęciach	• Wykład • Laboratorium
potrafi przeprowadzić proces usuwania zagrożeń w systemach i sieciach komputerowych	• K_W18 • K_U13 • K_U14	• dyskusja • kolokwium • obserwacja i ocena aktywności na zajęciach	• Wykład • Laboratorium
potrafi skonfigurować bezpieczną transmisję danych w sieciach WiFi	• K_U14	• kolokwium • obserwacja i ocena aktywności na zajęciach	• Laboratorium
rozumie potrzebę stosowania zabezpieczeń systemów i sieci komputerowych	• K_W18 • K_W19 • K_U14	• dyskusja • kolokwium	• Wykład • Laboratorium
rozumie konieczność pracy zespołowej przy uruchamianiu i monitorowaniu zabezpieczeń w rozbudowanych sieciach komputerowych	• K_W19 • K_U28 • K_K06	• dyskusja • kolokwium	• Wykład • Laboratorium
umie zdefiniować podstawową politykę bezpieczeństwa dla pojedynczego komputera i małej sieci komputerowej	• K_W18 • K_U14	• kolokwium	• Wykład • Laboratorium

Warunki zaliczenia

Wykład - warunkiem zaliczenia jest uzyskanie pozytywnych ocen z sprawdzianów wiedzy w formie pisemnej, przeprowadzonych co najmniej raz w semestrze

Laboratorium - warunkiem zaliczenia jest realizacja co najmniej 80% przewidzianych ćwiczeń laboratoryjnych i uzyskanie pozytywnych ocen ze sprawdzianów weryfikujących wiedzę i umiejętności zdobyte podczas ćwiczeń

Składowe oceny końcowej = wykład: 50% + laboratorium: 50%

Literatura podstawowa

1. C. W. Stallings, Kryptografia i bezpieczeństwo sieci komputerowych, Tomy 1-2, Helion, wyd. 4., 2019
2. McNab, Ocena bezpieczeństwa sieci, wyd.3, Helion, 2017
3. R. Boddington, Practical Digital Forensics, Packt, 2016
4. Lukatsky A.: Wykrywanie włamań i aktywna ochrona danych, Helion, 2004.

Literatura uzupełniająca

1. 1. S. McClure i in., Hacking zdemaskowany, PWN, 2005
2. Szmit, M. Gusta, M. Tomaszewski, 101 zabezpieczeń przed atakami w sieci komputerowej, Helion, 2005.
3. Kutyłowski M., Strothmann W.B.: Kryptografia. Teoria i praktyka zabezpieczania systemów komputerowych, Oficyna Wydawnicza Read ME, Warszawa, 1998.
4. Russell R. i in. : Hakerzy atakują. Jak przejąć kontrolę nad siecią, Helion, 2004.
5. Potter B., Fleck B.: 802.11. Bezpieczeństwo, Wyd. O'Reilly, 2005.
6. Balinsky A. i in.: Bezpieczeństwo sieci bezprzewodowych, PWN, CISCO Press, 2007.
7. Mochnacki W.: Kody korekcyjne i kryptografia. Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2000.
8. Schneider B.: Kryptografia dla praktyków — protokoły, algorytmy i programy zródłowe w języku C. Wydawnictwa Naukowo-Techniczne, Warszawa 1995.

Uwagi

Zmodyfikowane przez prof. dr hab. inż. Andrzej Obuchowicz (ostatnia modyfikacja: 20-04-2021 08:55)