KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Bezpieczeństwo systemów operacyjnych [S1Cybez1>BSO]

Przedmiot

Kierunek studiów
Cyberbezpieczeństwo

Rok/Semestr
3/6

Studia w zakresie (specjalność)
–

Profil studiów
ogólnoakademicki

Poziom studiów
pierwszego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład
16

Laboratorium
30

Inne
0

Ćwiczenia
0

Projekty/seminaria
12

Liczba punktów ECTS

4,00

Koordynatorzy

dr inż. Marek Michalski
marek.michalski@put.poznan.pl

dr hab. inż. Mariusz Żal
mariusz.zal@put.poznan.pl

Wykładowcy

Wymagania wstępne

Student przystępujący do zajęć powinien posiadać wiedzę w zakresie architektury komputerów oraz systemów operacyjnych, sieci komputerowych, podstaw IoT oraz podstaw krytpografii. Powinien też posiadać umiejętność programowania w językach wysokiego poziomu.

Cel przedmiotu

Celem przedmiotu jest zapoznanie studentów z typowymi zagrożeniami i atakami na system operacyjny. W trakcie zajęć studenci poznają różne techniki zabezpieczania systemów operacyjnych, dotyczącę zarówno sprzętu jak i oprogramowania. Poznają równonież metody ataku na system operacyjny jak rónież techniki obrony.

Przedmiotowe efekty uczenia się

Wiedza:
Ma wiedzę w zakresie funkcji sieciowych realizowanych przez system operacyjny, w tym ich

bezpieczeństwa [K1_W07]
Zna rodzaje ataków na systemy operacyjne [K1_W10]
Rozumie zagrożenia, na które narażona jest współczesna cywilizacja masowa korzystająca z usług cyfrowych, w których to systemy operacyjne odgrywają istotną rolę [K1_W20]

Umiejętności:
Potrafi korzystać ze źródeł literaturowych, integrować pozyskane informacje, oceniać je oraz dokonywać ich interpretacji i wyciągać wnioski, w celu rozwiązania złożonych i nietypowych problemów w obszarze cyberbezpieczeństwa [K1_U01]
Potrafi dobrać metody zabezpieczeń do rodzaju systemu operacyjnego oraz tego, jakie funkcje pełni [K1_U02]
Potrafi porównać różne rodzaje zabezpieczeń i techniki uwierzytelniania w celu dobru rozwiazania zapewniającego bezpieczeństwo systemów operacyjnych [K1_U08]

Kompetencje społeczne:
Rozumie znaczenie podnoszenia kompetencji zawodowych, osobistych i społecznych; ma świadomość, że wiedza i umiejętności w obszarze cyberbezpieczeństwa szybko ewoluują [K1_K01]
Jest świadomy opowiedzialnośc za wdrażane rozwiazania i potrafi pracować w grupie [K1_K05]

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:
Wiedza zdobyta w ramach wykładu weryfikowana jest przez egzamin w formie pisemnej lub ustnej. W formie pisemnej studenci muszą udzielić odpowiedzi na 7 - 10 pytań (testowych i otwartych) różnie punktowanych. Są trzy lub cztery grupy punktowe. Natomiast w przypadku egzaminu ustnego student losuje po jednym pytaniu z każdej grupy punktowej. W formie ustnej, do każdego wylosowanego pytania, student może otrzymać dodatkowe pytanie (związane z wylosowanym pytaniem). Ocena pytania (obejmuje odpowiedź zarówno na pytanie wylosowane jak i pytanie dodatkowe) obejmuje zakres odpowiedzi oraz głębię zrozumienia zagadnienia. Do każdego egzaminu przygotowywanych jest 50 - 60 pytań. Warunkiem pozytywnego zaliczenia egzaminu otrzymanie minimum 50% punktów możliwych do zdobycia.
Umiejętności nabyte w ramach projektów oceniane są na podstawie prezentowanych projektów. Ocenie poddawane jest zaangażownie w przygotwanie projektu, wykorzystane narzędzia oraz zakres dodatkowej wiedzy, jaką studneci musieli posiąść. Projekty są jedno lub dwuosobowe. Skala ocen 2 - 5.
Umiejętności nabyte w ramach laboratorium weryfikowane są na podstawie zadania realizowanego na ostatnich zajęciach. Zadanie podzielny jest na 5 - 6 podzadań różnie punktowanych. Podzadania stanowią całość, możliwe jest jednak niezależne ich wykonanie. Brak wykonania podzadania nie wpływa na ocenę pozostałych podzadań. Próg zaliczeniowy: 50% punktów.
Kryteria oceny egzaminu i zaliczania (laboratoria):
liczba punktów ocena
<=50 % 2,0
51% - 60% 3,0
61% - 70% 3,5
71% - 80% 4,0
81% - 90% 4,5
91% - 100% 5,0
Dodatkowo zasady zaliczania przedmiotu i dokładne progi zaliczeniowe zostaną przekazane studentom na początku semestru z wykorzystaniem uczelnianych systemów elektronicznych oraz na pierwszych zajęciach (w każdej formie zajęć).

Treści programowe

Program zajęć obejmuje aspekty bezpieczeństwa systemów operacyjnych w zakresie sprzętu, jak również oprogramownia. Prezentowane treści uwzględniają również wpływ użytkownika na bezpieczeństwo systemów operacyjnych.

Tematyka zajęć

Wykłady:

1. Wprowadzenie do bezpieczeństwa systemów operacyjnych
2. Bezpieczeństwo architektury systemu operacyjnego
3. Kontrola dostępu i uprawnień
4. Uwierzytelnianie i autoryzacja użytkowników
5. Metody kryptograficzne stosowane w systemach operacyjnych
6. Ochrona przed złośliwym oprogramowaniem
7. Konfiguracja systemu operacyjnego
8. Bezpieczeństwo usług sieciowych w systemach operacyjnych
9. Rejestracja zdarzeń, analiza powłamaniowa i reagowanie na incydenty
10. Standardy, normy i polityki bezpieczeństwa
Laboratoria:
Tematyka zajęć zgodna z treściami wykładów.
Projekty:
Projekty realizowane w grupach jedno- lub dwuosobowych. Tematy projektów zgodne z tematami wykładów.

Metody dydaktyczne

Wykład - prezentacje multimedialne ilustrowane przykładami podawanymi na tablicy.
Ćwiczenia laboratoryjne - wykonywanie zadań podanych przez prowadzącego zupełniane prezentacjami multimedialnymi.
Zajecia projektowe - prezentacja multimedialne, dyskusje ze studentami.

Literatura

Podstawowa:
1. Abraham Silberschatz, Greg Gagne, Peter B. Galvin, Podstawy systemów operacyjnych tom 1, 2 i 3. Wydawnictwo Naukowe PWN, 2021.
2. Donald A. Tevault, Bezpieczeństwo systemu Linux. Hardening i najnowsze techniki zabezpieczania przed cyberatakami, Wydawnictwo Helion, 2024.

Uzupełniająca:
Uzupełniająca
1. Forshaw James, Windows Security Internals: A Deep Dive Into Windows Authentication, Authorization, and Auditing, No Starch Pr, 2024

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	103	4,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	58	2,50
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	45	1,50