Sylabus przedmiotu / modułu kształcenia	
Nazwa przedmiotu/modułu kształcenia:	**Bezpieczeństwo systemów komputerowych**
Nazwa w języku angielskim:	Computer security
Język wykładowy:	polski
Kierunek studiów, dla którego przedmiot jest oferowany:	informatyka
Jednostka realizująca:	Instytut Informatyki
Rodzaj przedmiotu/modułu kształcenia (obowiązkowy/fakultatywny):	obowiązkowy
Poziom modułu kształcenia (np. pierwszego lub drugiego stopnia, jednolitych magisterskich):	pierwszego stopnia
Rok studiów:	trzeci
Semestr:	piąty
Liczba punktów ECTS:	3
Imię i nazwisko koordynatora przedmiotu:	dr Piotr Świtalski
Imię i nazwisko prowadzących zajęcia:	dr Piotr Świtalski, mgr Dominik Filipczuk
Założenia i cele przedmiotu:	Założeniem tego przedmiotu jest znajomość przez słuchaczy zagadnień związanych z podstawami architektury komputerów, systemami operacyjnymi oraz sieciami komputerowymi. Wskazana jest również wiedza dotycząca protokołów warstwy aplikacji w stosie sieciowym. Celem przedmiotu jest zaznajomienie studentów z problematyką bezpieczeństwa systemów komputerowych, m.in.: ● podstawami szyfrów oraz zasadami tworzenia i weryfikacji podpisu cyfrowego, ● znanymi atakami wymierzonymi w systemy komputerowe, ● metodami przeciwdziałania atakom i zabezpieczania systemów komputerowych.

Symbol efektu	**Efekty uczenia się**	**Symbol efektu kierunkowego**
	WIEDZA **Student zna i rozumie:**	
W_01	podstawowe techniki szyfrowania danych oraz zagadnienia z zakresu tworzenia i weryfikacji podpisu cyfrowego	**K_W05**
W_02	mechanizmy uwierzytelniania użytkownika w systemach komputerowych	**K_W05, K_W07**
W_03	metody przeprowadzania ataków wymierzonych w systemy komputerowe	**K_W05, K_W11**
W_04	zasady zabezpieczania sieci komputerowych oraz wykrywania anomalii w tych sieciach	**K_W07**
	UMIEJĘTNOŚCI **Student potrafi:**	
U_01	sprawnie wyszukiwać w dokumentacji producenta istotne parametry i tryby pracy aplikacji służącej do zabezpieczenia systemu	**K_U01**
U_02	sprawnie wykorzystać narzędzia bezpieczeństwa systemów komputerowych	**K_U15, K_U17**
U_03	dobrać adekwatne zabezpieczenia w stosunku do zagrożenia w systemie komputerowym	**K_U15, K_U17, K_U25**

Forma i typy zajęć:	studia stacjonarne: wykłady (30 godz.), ćwiczenia laboratoryjne (30 godz.) studia niestacjonarne: wykłady (15 godz.), ćwiczenia laboratoryjne (15 godz.)

Wymagania wstępne i dodatkowe:

Warunkiem uczestnictwa w zajęciach jest uprzednie zaliczenie następujących przedmiotów: „Architektura systemów komputerowych”, „Systemy operacyjne”, „Podstawy technologii WWW”, „Sieci komputerowe” lub znajomość literatury obowiązującej w tych przedmiotach.

Treści modułu kształcenia:

Treści dotyczące wykładu:

1. **Koncepcja bezpieczeństwa komputerowego.** Podstawowe zasady. Właściwości i klasyfikacja koncepcji bezpieczeństwa: integralność, dostępność, poufność, niezaprzeczalność, odpowiedzialność. Podstawowe pojęcia. Model bezpieczeństwa sieciowego. Minimalne standardy bezpieczeństwa. Polityka bezpieczeństwa.
2. **Ataki w systemach komputerowych.** Specyfika systemów informatycznych. Klasyfikacja zagrożeń. Szkodliwe oprogramowanie. Sieci botnet. Ataki na współczesne procesory. Statystyka typowych zagrożeń. Przestępstwa ujawnione i nieujawnione. Obiekty, typy i sprawcy przestępstw. Piractwo komputerowe, sabotaż, wywiad gospodarczy, szpiegostwo, przestępstwa bankowe. Inżynieria społeczna. Phising. Inżynieria odwrotna. Organizacje przeciwdziałające przestępczości komputerowej.
3. **Szkodliwe oprogramowanie.** Problemy związane z nieautoryzowanym dostępem do systemów komputerowych. Infekcje systemów komputerowych. Bezpieczny system operacyjny. Podatność systemów operacyjnych. Charakterystyka szkodliwego oprogramowania: tylne drzwi, bomby logiczne, konie trojańskie, wirusy, robaki, eksploity i rootkity, keyloggery. Przeciwdziałanie szkodliwemu oprogramowaniu.
4. **Klasyczne techniki szyfrowania.** Dziedzina kryptografii i podstawowe pojęcia. Podstawowe techniki szyfrowania: technika podstawieniowa, szyfr Cezara, szyfry mono i polialfabetyczne, szyfr Playfaira, szyfr Vigenère'a. Techniki przestawieniowe, szyfr zygzakowy, maszyny wirnikowe. Szyfrowanie symetryczne. Ataki siłowe przeprowadzane na algorytmy szyfrowania.
5. **Współczesne szyfry komputerowe.** Szyfry strumieniowe. Szyfr strumieniowy RC4. Szyfry blokowe. Struktura i szyfr Feistela. Standard DES, efekt lawiny. Algorytm AES. Tryby operacyjne szyfrów blokowych. Szyfrowanie asymetryczne. Algorytm RSA.
6. **Podpis cyfrowy.** Idea podpisu cyfrowego. Wymagania stawiane podpisom cyfrowym. Mechanizm uwierzytelniania komunikatów. Kody uwierzytelnienia komunikatów MAC. Podpis cyfrowy ElGamal. Standard DSS. Algorytm DSA. Kryptograficzne funkcje haszujące. Algorytm SHA-512. Paradoks urodzin.
7. **Uwierzytelnianie.** Pojęcie uwierzytelniania. Uwierzytelnianie przez hasło. Strategie wyboru haseł. Inne metody uwierzytelniania. Protokoły uwierzytelniania: protokół challenge and response. Atak „człowiek pośrodku”. Dowód z wiedzą zerową. Uwierzytelnianie wieloskładnikowe. Hasło jednorazowe. Generowanie haseł jednorazowych – protokół S/KEY.
8. **Kontrola dostępu.** Zasady kontroli dostępu. Podmiot, obiekt i prawa dostępu. Kontrola dostępu uznaniowa (DAC). Kontrola dostępu bazująca na rolach (RBAC). Kontrola dostępu bazująca na atrybutach (ABAC). Przykład kontroli dostępu: SELinux.

9. **Protokoły i standardy bezpieczeństwa w Internecie.** Bezpieczeństwo poczty elektronicznej. S/MIME. Protokoły SSL/TLS. Ataki na protokoły TLS. Protokół HTTPS. Nagłówki w protokole HTTP. Architektura IPsec.
10. **Zapory sieciowe (firewalle).** Model ogólny zapory sieciowej. Charakterystyka firewalli. Ograniczenia firewalli. Firewall filtrujący pakiety. Firewall filtrujący pakiety z badaniem stanu pakietu. Brama aplikacyjna, brama transmisyjna. Implementacja firewalla. Strefa zdemilitaryzowana (DMZ). Przykładowa konfiguracja firewalla z DMZ.
11. **Systemy wykrywania intruzów.** Zachowania intruzywne. Wzorce zachowań intruzów. Wykrywanie intruzów. Statystyczna analiza zachowania. Wykrywanie intruzów w oparciu o reguły. Systemy IDPS. Audyt w systemach IDPS. Pułapki (Honeypoty).
12. **Bezpieczeństwo aplikacji internetowych cz. 1.** Ataki w warstwie aplikacji. Niewłaściwa kontrola dostępu do aplikacji. Błędy kryptograficzne. Wstrzykiwanie kodu. Ataki SQL Injection. Atak XSS. Atak CSRF.
13. **Bezpieczeństwo aplikacji internetowych cz. 2.** Niebezpieczne projektowanie. Błędy w konfiguracji oprogramowania. Błędy w uwierzytelnianiu użytkownika i zarządzania jego sesją. Niewłaściwe zabezpieczenie wrażliwych danych. Awarie oprogramowania. Niewystarczające logowanie i monitorowanie aplikacji. Atak SSRF.
14. **Bezpieczeństwo systemów mobilnych.** Model izolowania procesów. Piaskownica. Uprawnienia Androida. Android Package. Manifest aplikacji i integralność pakietu. Weryfikacja manifestu. Zagrożenia i podatności w aplikacjach mobilnych. Ewolucja złośliwego oprogramowania w systemach mobilnych. Ataki na sprzęt. Bezpieczeństwo urządzeń mobilnych. Technologie zarządzania urządzeniami mobilnymi.
15. **Zapewnianie dostępności danych.** Utrzymanie ciągłości zasilania. Sposoby zapobiegania problemom zasilania, zasilacze awaryjne UPS. Ochrona danych przed utratą. Systemy macierzowe RAID. Kopie bezpieczeństwa.

Treści dotyczące laboratorium:

1. **Podsłuchiwanie ruchu sieciowego.** Podsłuchiwanie ruchu ICMP, przechwytywanie danych połączenia telnet, analiza pakietów dla ruchu SSH.
2. **Bezpieczeństwo w systemach operacyjnych cz. 1**. Zarządzanie kontami i grupami użytkowników w systemie Windows. Inspekcja. Rejestr systemu Windows. Wykrywanie potencjalnych zagrożeń.
3. **Bezpieczeństwo w systemach operacyjnych cz. 2**. Zarządzanie użytkownikami systemu Linuks. Postarzanie haseł. Polecenia sudo i su. Bity SUID i GUID. Aktualizacja systemu Linuks.
4. **Eksploitowanie systemu Windows**. Konfiguracja środowiska testowego dla Metasploita. Wykorzystanie eksploita. Instalacja backdoora i keyloggera.
5. **Szyfrowanie danych cz. 1 - szyfry i ich łamanie**. Entropia. Szyfr Cezara. Szyfr przestawieniowy.
6. **Szyfrowanie danych cz. 2 – szyfry asymetryczne i podpis cyfrowy**. Generowanie kluczy: prywatnego i publicznego. Tworzenie certyfikatu CA. Tworzenie i podpisanie certyfikatu użytkownika. Konfiguracja serwera HTTP dla bezpiecznej wymiany danych przez SSH.
7. **Funkcje haszujące**. Długość generowanych wyników funkcji haszujących. Badanie własności funkcji haszujących. Solenie. Łamanie haszy za pomocą narzędzia hashkiller.io. Szybkość obliczania haszy. Funkcja HMAC.

8. **Łamanie haseł.** Sposoby przechowywania haseł kont użytkowników w SO. Programy wykorzystywane do łamania haseł: John the Ripper i hashcat. Łamanie haseł systemu Windows. Łamanie haseł systemu Linuks. Łamanie haszy w programie hashcat.
9. **Atak Man in the Middle (MitM).** Konstrukcja ataku. Atak MitM wymierzony w użytkownika przeglądarki internetowej. Przeprowadzenie ataku MitM w środowisku kontenerów.
10. **SELinux.** Wprowadzenie do SELinux. Narzędzia SELinux. Polityka SELinux. Kontekst bezpieczeństwa.
11. **Zapora sieciowa**. Zasady tworzenia reguł dla firewalla iptables. Przykłady reguł iptables. Konfiguracja zapory sieciowej. Filtrowanie pakietów przychodzących. Filtrowanie według adresu IP oraz MAC. Logowanie odrzuconych pakietów.
12. **System wykrywania intruzów**. Przygotowanie środowiska testowego. Tryby pracy Snorta. Tworzenie reguł użytkownika. Tworzenie reguł związanych z atakami.
13. **Ataki na aplikacje internetowe cz. 1**. Przygotowanie środowiska testowego. Atak trwały XSS. Atak odbity XSS. Atak XSS bazujący na obiektach DOM. Atak Cross Site Request Forgery (CSRF). Atak SQL Injection.
14. **Ataki na aplikacje internetowe cz. 2**. Atak Blind SQL Injection. Podatność na ataki związane z przesyłaniem plików. Powłoki wielofunkcyjne. Powłoka odwrotna. Złośliwe pliki SVG. Obejście zabezpieczenia na podstawie rozszerzeń. Obejście zabezpieczenia na podstawie typu MIME.
15. **Kopie bezpieczeństwa.** Program rsync. Kopia przyrostowa w rsync. Automatyzacja procesu tworzenia kopii bezpieczeństwa.

Literatura podstawowa:

1. Stallings W., Brown L.: Bezpieczeństwo systemów informatycznych. Zasady i praktyka, Wydanie IV. Tom 1, Wyd. Helion, Gliwice, 2023.
2. Khawaja G.: Kali Linux i testy penetracyjne. Biblia. Wyd. Helion, Gliwice, 2022.

Literatura dodatkowa:

1. Stallings W., Brown L.: Bezpieczeństwo systemów informatycznych. Zasady i praktyka, Wydanie IV. Tom 2, Wyd. Helion, Gliwice, 2023.
2. Janca T.: Alicja i Bob. Bezpieczeństwo aplikacji w praktyce. Wyd. Helion, Gliwice, 2021.
3. Tevault D. A.: Bezpieczeństwo systemu Linux. Hardening i najnowsze techniki zabezpieczania przed cyberatakami, Wyd. Helion, Gliwice, 2024.

Planowane formy/działania/metody dydaktyczne:

Wykład tradycyjny wspomagany jest technikami multimedialnymi. Ćwiczenia laboratoryjne – zajęcia praktyczne z wykorzystaniem wybranych narzędzi programowych. Na stronie internetowej prowadzącego zamieszczane są materiały z problemami i zadaniami laboratoryjnymi.

Sposoby weryfikacji efektów uczenia się osiąganych przez studenta:

Symbol efektu	Metody weryfikacji efektów uczenia się
W_01	Efekt realizowany na egzaminie w formie pisemnej. Przykładowe pytanie: „Jak weryfikowany jest podpis cyfrowy?”.
W_02	Efekt realizowany na egzaminie w formie pisemnej. Przykładowe pytanie: „Jakiego rodzaju składnik materialny może być użyty w uwierzytelnianiu wieloskładnikowym (MFA)?”.

W_03	Efekt realizowany na egzaminie w formie pisemnej. Przykładowe pytanie: „W jaki sposób przeprowadzany jest atak DDoS?”.
W_04	Efekt realizowany na egzaminie w formie pisemnej. Przykładowe pytanie: „Przedstaw statystyczną analizę zachowania w systemach IDPS”.
U_01	Efekt realizowany w trakcie zajęć laboratoryjnych. Sprawdzane będą umiejętności korzystania z dokumentacji danego rozwiązania. Przykładowe zadanie: „Sprawdź w dokumentacji programu selinux jak można zweryfikować prawidłowość kontekstu danego pliku względem jego położenia w systemie plików”.
U_02	Efekt realizowany w trakcie zajęć laboratoryjnych. Sprawdzane będą umiejętności konfiguracji zabezpieczeń w systemie komputerowym. Przykładowe zadanie: „Wygeneruj i zaimplementuj certyfikat SSL w wybranym serwerze HTTP”.
U_03	Efekt realizowany w trakcie zajęć laboratoryjnych. Student będzie realizował zadanie związane z instalacją i konfiguracją określonego zabezpieczenia. Przykładowe zadanie: „Zabezpiecz usługi systemu operacyjnego Linuks przy pomocy wybranej zapory sieciowej.

Forma i warunki zaliczenia:

Moduł kończy się egzaminem. Ocena z przedmiotu składa się z dwóch ocen cząstkowych:

- oceny z zajęć laboratoryjnych,
- oceny z egzaminu końcowego.

Na ocenę z zajęć laboratoryjnych składają się oceny cząstkowe uzyskane na regularnych zajęciach z nauczycielem akademickim, za które można uzyskać sumarycznie 50 pkt. Zaliczenie zajęć laboratoryjnych możliwe po uzyskaniu co najmniej 51% liczby punktów z tej formy zaliczenia

Egzamin jest egzaminem pisemnym. Do egzaminu mogą przystąpić osoby, które uzyskały zaliczenie laboratorium. Na egzaminie można uzyskać maksymalnie 50 pkt. Egzamin będzie zaliczony w przypadku uzyskania co najmniej 51% liczby punktów z tej formy zaliczenia.

Ocena końcowa, w zależności od sumy uzyskanych punktów (maksymalnie 100 pkt) jest następująca (w nawiasach ocena wg skali ECTS):

- 0 – 50 pkt: niedostateczna (F),
- 51 – 60 pkt: dostateczna (E),
- 61 – 70 pkt: dostateczna plus (D),
- 71 – 80 pkt: dobra (C),
- 81 – 90 pkt: dobra plus (B),
- 91 – 100 pkt: bardzo dobra (A).

Bilans punktów ECTS:

Studia stacjonarne

Aktywność	Obciążenie studenta
Udział w wykładach	30 godz.
Udział w ćwiczeniach laboratoryjnych	30 godz.
Przygotowanie się do egzaminu	6 godz.
Obecność na egzaminie	1 godz.
Przygotowanie się do ćwiczeń laboratoryjnych	6 godz.

Udział w konsultacjach z przedmiotu	2 godz.
Sumaryczne obciążenie pracą studenta	**75 godz.**
Punkty ECTS za przedmiot	**3 ECTS**

Studia niestacjonarne	
Aktywność	Obciążenie studenta
Udział w wykładach	15 godz.
Udział w ćwiczeniach laboratoryjnych	15 godz.
Przygotowanie się do egzaminu	21 godz.
Obecność na egzaminie	1 godz.
Przygotowanie się do ćwiczeń laboratoryjnych	21 godz.
Udział w konsultacjach z przedmiotu	2 godz.
Sumaryczne obciążenie pracą studenta	**75 godz.**
Punkty ECTS za przedmiot	**3 ECTS**