Autor*: dr hab. inż. Krzysztof Szczypiorski, prof. PW*

Wprowadzenie do Cyberbezpieczeństwa (WCYBER)
Introduction to Cybersecurity

Poziom kształcenia: I stopień
Forma i tryb prowadzenia przedmiotu: stacjonarna
Kierunek studiów: Cyberbezpieczeństwo
Specjalność:
Grupa przedmiotów:
Poziom przedmiotu: podstawowy
Status przedmiotu: obowiązkowy
Język przedmiotu: polski
Semestr nominalny (tylko dla przedmiotów obowiązkowych): 1
Minimalny numer semestru: 1
Wymagania wstępne, zalecane przedmioty poprzedzające: n/d
Limit liczby studentów: 60

Powód zgłoszenia przedmiotu: program studiów na nowym kierunku Cyberbezpieczeństwo

Cel przedmiotu:

Głównym celem przedmiotu jest wprowadzenie studentów do dziedziny inżynierii cyberbezpieczeństwa. W ramach przedmiotu omówione zostaną fundamentalne zagadnienia dotyczące bezpieczeństwa sieci, systemów i użytkowników wzajemnie na siebie oddziałowujących w świecie cyfrowym. Kontekstem wprowadzenia tych zagadnień będzie metodyka modelowania zagrożeń w cyberprzestrzeni poprzez identyfikację Łańcucha Śmierci (ang. Kill Chain). W dalszej kolejności zostanie dokonany przegląd głównych obszarów zapewniania bezpieczeństwa w cyberprzestrzeni. Każdy obszar zostanie scharakteryzowany właściwymi środkami technicznymi i nietechnicznymi. Ponadto przedmiot stanowi orientację dla przyszłych inżynierów cyberbezpieczeństwa – absolwentów kierunku Cyberbezpieczeństwo.

Założeniem prowadzenia przedmiotu jest ukierunkowanie się na naukę praktyczną. Zajęcia wykładowe będą w większości poświęcone studiowaniu rzeczywistych sytuacji, w których realizują się omawiane zagadnienia. Zajęcia laboratoryjne będą oparte o wykonywanie praktycznych zadań inżynierskich ilustrujących zagadnienia wykładowe. Celem laboratorium jest praktyczne wprowadzenie studentów do systemowej inżynierii cyberbezpieczeństwa. Zadania laboratoryjne będą dotyczyły pozyskiwania informacji o sieci, systemach i użytkownikach, testowania ich bezpieczeństwa oraz zarządzania bezpieczeństwem cyberprzestrzeni z wykorzystaniem wirtualnego środowiska sieci, systemów i użytkowników. W ramach zajęć projektowych studenci będą realizować zadanie typu *studium przypadku na żywo* z zakresu projektowania procesów zarządzania incydentami naruszeń bezpieczeństwa sieci, systemów i użytkowników. Ponadto przygotują krytyczną analizę materiałów źródłowych z zakresu zagadnień cyberbezpieczeństwa.

Treść kształcenia:

WYKŁADY:

1. **Systemy cyber-fizyczne, cyberprzestrzeń i cyberbezpieczeństwo (2 godz.)**
   Cyberprzestrzeń; sieci, systemy i użytkownicy; systemy cyber-fizyczne; modelowanie systemów; współczesne sieci i systemy; trendy; Wprowadzenie do dziedziny cyberbezpieczeństwa; Co to znaczy „zajmuję się cyberbezpieczeństwem?", w kontekście: technicznym, naukowym, biznesowym, prawnym, ekonomicznym; Model obszarów cyberbezpieczeństwa – zagadnienia, kompetencje i zawody; Cyberbezpieczeństwo a bezpieczeństwo cybernetyczne;

2. **Podstawowe zagadnienia z dziedziny cyberbezpieczeństwa (2 godz.)**
   Pojęcia fundamentalne dla dziedziny – CIA (Confidentiality, Integrity, Availability); podatność, zagrożenie, skutek, ryzyko; Systemowego podejście do cyberbezpieczeństwa; Modelowanie zagrożeń i ocena ryzyka; Podejście klasyczne do modelowania zagrożeń; Nowe metodyki modelowania i testowania bezpieczeństwa w kontekście Advanced Persisent Threats; Wprowadzenie do modelowania bezpieczeństwa cyberprzestrzeni metodyką *Kill Chain*;

3. **Zagrożenia w cyberprzestrzeni – metodyka Kill Chain: Rekonesans (2 godz.)**
   Pozyskiwanie informacji o celach – podejścia, techniki, biały wywiad; wprowadzenie do wyszukiwania podatności (Vulnerability Assesment) sieci i systemów; Planowanie ataków – podejścia, techniki, wektory ataku; Wpływ ataków; Metody in

4. **Zagrożenia w cyberprzestrzeni – metodyka Kill Chain: Techniki przygotowywania ataków i przełamywania zabezpieczeń; dystrybucja malware (2 godz.)**
   Złośliwe oprogramowanie (malware): rodzaje, podstawowe pojęcia, architektura; Metody dystrybucji złośliwego oprogramowania, w tym odniesienie do socjotechniki; Warsztat analityka malware; Wprowadzenie do klasycznych technik detekcji i analizy malware; Nowe techniki detekcji i analizy malware; Techniki unikania detekcji i utrudniania analizy malware;

5. **Zagrożenia w cyberprzestrzeni – metodyka Kill Chain: Eksploitacja systemów, utrzymywanie dostępu i sterowanie atakami (2 godz.)**
   Podstawowe techniki przełamywania zabezpieczeń systemów operacyjnych i systemów komputerowych; Przejmowanie kontroli i wykonywanie arbitralnego oprogramowania; Techniki utrzymywania złośliwego oprogramowania w systemie; Tylne furtki; Sieci Malware, czyli botnety: podstawowe pojęcia, elementy, architektura; Komunikacja i sterowanie atakami;

6. **Zagrożenia w cyberprzestrzeni – metodyka Kill Chain: Ataki – case studies. (2 godz.)**
   Cele atakujących; Trendy i case study: ransomware, IoT botnets, cryptojacking, steganografia, botnet-as-a-service; Cyber Warfare; grupy APT i ich metody działania; Wpływ społeczno-ekonomiczny ataków w cyberprzestrzeni; prawo a cyberprzestępstwa; etyka a cyberprzestrzępstwa;

7. **Metody i środki obrony przed współczesnymi atakami na sieci, systemy i użytkowników: bezpieczeństwo systemów i oprogramowania (4 godz.)**
   Mechanizmy bezpieczeństwa w systemach: uwierzytelnienie, kontrola dostępu; Polityki bezpieczeństwa; Monitorowanie, utrzymywanie i odzyskiwanie systemów; Projektowanie, modelowanie, testowanie, audyt systemów i oprogramowania w kontekście cyberbezpieczeństwa; Test penetracyjny, audyt bezpieczeństwa; Etapy testu penetracyjnego, techniki i warsztat pentestera; Tworzenie raportu z pentestów; Red Teaming, Blue Teaming, Purple Teaming; Inżynieria odwrotna;

8. **Metody i środki obrony przed współczesnymi atakami na sieci, systemy i użytkowników: bezpieczeństwo danych (4 godz.)**
   Kryptografia i kryptoanaliza; Integralność i autentyczność danych; Kontrola dostępu; Protokoły bezpiecznej komunikacji; Bezpieczeństwo przechowywania danych; Prywatność; Zastosowanie kryptografii w bezpieczeństwie systemów;

9. **Metody i środki obrony przed współczesnymi atakami na sieci, systemy i użytkowników: bezpieczeństwo komunikacji (2 godz.)**
   Dobre praktyki zabezpieczenia sieci teleinformatycznych; sprzęt i oprogramowanie dla bezpieczeństwa teleinformatycznego: IDS/IPS, firewall, secure gateways, systemy kontroli dostępu, systemy bezpiecznej łączności; monitoring komunikacji sieciowej; analiza ruchu sieciowego dla cyberbezpieczeństwa; honeypots/honeynets; aplikacje analityczne, systemy SIEM;

10. **Metody i środki obrony przed współczesnymi atakami na sieci, systemy i użytkowników: kryminalistyka cyfrowa (4 godz.)**
    Pojęcia podstawowe; Pozyskiwanie danych śledczych z urządzeń cyfrowych: metody, zabezpieczanie materiału dowodowego, praca z materiałem dowodowym, akwizycja danych; Pozyskiwanie danych śledczych jako strumieni komunikacji: kontekst sieci, systemów i użytkowników, przechwytywanie i analiza sieciowych strumieni komunikacji, przechwytywanie i analiza danych cyfrowych; techniki poszukiwań atakujących: biały wywiad, Dark Web, wywiad gospodarczy; Digital Forensics jako element zarządzania cyberbezpieczeństwem; Aspekty prawne dochodzenia śledczego z dowodami cyfrowymi; metody kryminalistyki cyfrowej w kontekście prywatnym, compliance, spory prywatne;

11. **Metody i środki obrony przed współczesnymi atakami na sieci, systemy i użytkowników: bezpieczeństwo organizacyjne, społeczne i zarządzanie cyberbepieczeństwem. (2 godz.)**

Organizacja systemów bezpieczeństwa i zarządzanie incydentami; zarządzanie ryzykiem; strategia i planowanie polityk bezpieczeństwa organizacji; Zarządzanie ryzykiem; Threat Intelligence i bezpieczeństwo oparte o analitykę danych; Zarządzanie tożsamością użytkowników i systemów; inżyniera społeczna; prywatność zachowania i danych użytkowników; normy w zakresie cyberbezpieczeństwa.

12. Podsumowanie (2 godz.)

Cyberbezpieczeństwo sieci, systemów i użytkowników jako wielowymiarowy proces; podsumowanie przedmiotu jako analizy bezpieczeństwa cyberprzestrzeni metodyką Kill Chain; metody zarządzania obroną przed atakiem typu APT: rodzaje reakcji na poszczególne ataki, formułowanie strategii koncentrującej się na coraz wcześniejszym przerywaniu łańcucha; orientacja rozwoju kompetencji inżyniera cyberbezpieczeństwa na kierunku Cyberbezpieczeństwo;

ĆWICZENIA:

–

LABORATORIA:

W ramach projektu każdy student będzie miał do wykonania 4 zadania praktyczne posiłkując się instruktażem Prowadzącego w zakresie:

1) Metody pozyskiwania informacji: rekonesans, skanowanie, biały wywiad, threat intelligence, vulnerability assesment
2) Testowanie bezpieczeństwa danych, aplikacji i systemów z wykorzystaniem specjalistycznych narzędzi;
3) Elementy analizy złośliwego oprogramowania;
4) Wykorzystanie wirtualnej sieci komputerowej do wykonania ćwiczeń związanych zapewnianiem bezpieczeństwa cyberprzestrzeni. Realizacja zadania będzie obejmowała monitorowanie sieci i systemów, implementację mechanizmów bezpieczeństwa sieci i systemów oraz modelowania i symulowania zagrożeń w celu przetestowania wprowadzonych mechanizmów i zebrania dowodów wykonania ataków;

Na każde ćwiczenie przewiduje 4 godziny pracy studenta.

PROJEKT:

W ramach projektu zespoły 4-osobowe będzie miał do wykonania zadanie w postaci *„Studium przypadku na żywo”*. Zespoły otrzymają zadanie do rozwiązania z zakresu zarządzania incydentami naruszeń bezpieczeństwa komputerowego. Zadanie to będzie zwieńczone prezentacją i demonstracją tworzoną w trakcie zajęć.

Ponadto elementem projektu będzie wykonanie przez każdego studenta przedmiotu krytycznego przeglądu literatury naukowej, technicznej i biznesowej z zakresu zagadnień cyberbezpieczeństwa zwieńczonego raportem.

Treść kształcenia - streszczenie w jęz. angielskim:

The main objective is to introduce students to the field of cyber security engineering. The course discusses fundamental issues related to the security of networks, systems and users that interact with each other in the digital world. The context of introducing these issues is the methodology of modeling threats in cyberspace by identifying the Kill Chain. Next, the main areas of ensuring security in cyberspace are reviewed. Each area of cybersecurity is characterized by appropriate technical and non-technical measures. In addition, the is an orientation for future cyber security engineers - graduates of Cybersecurity.

Egzamin: NIE

Literatura i oprogramowanie:

Materiały do zajęć – slajdy, opracowania, artykuły

Książki:

1. A. J. White, B. Clark: Blue Team Field Manual; 2017; CreateSpace Independent Publishing Platform; ISBN 978-1541016361
2. B. Clark: Red Team Field Manual; 2014; CreateSpace Independent Publishing Platform; ISBN 978-1494295509
3. A. Harper et al.: Gray Hat Hacking: The Ethical Hacker's Handbook, 5th Ed.; 2018; McGraw-Hill Education; ISBN 978-1260108415
4. J. Luttgens, M. Pepe, K. Mandia: Incident Response & Computer Forensics, 3rd Ed.; 2014; McGraw-Hill Education; ISBN 978-0071798686
5. SP 800-61: Computer Security Incident Handling Guide; Rev.2; 2012; US NIST
6. C. Hadnagy: Social Engineering: The Art of Human Hacking; John Wiley & Sons; 1 edition (17 Dec. 2010), ISBN: 978-0470639535

Oprogramowanie:

- Systemy operacyjne Windows, Linux, macOS – wersje klienckie i serwerowe;
- Oprogramowanie open source i komercyjne do realizacji zadań praktycznych z zakresu przedmiotu:
    - emulacji sieci i systemów;
    - narzędzia do analizy, detekcji cyber zagrożeń;
    - narzędzia do monitoringu systemów, sieci i użytkowników;
    - narzędzia do wykonywania aktywnych testów bezpieczeństwa systemów, sieci i użytkowników;

Wymiar godzinowy zajęć:	W	C	L	P
	30	–	15	15

Przewidywane formy kształcenia i organizacja przedmiotu

Realizacja przedmiotu obejmuje następujące formy zajęć:

– wykład prowadzony w wymiarze 2 godz. tygodniowo,

- zajęcia laboratoryjne; w ramach tych zajęć student, korzystając z oprogramowania i sprzętu będzie realizował wskazane zadania związane z monitorowaniem sieci i systemów, modelowaniem, symulowaniem i wykrywaniem zagrożeń oraz testów penetracyjnych systemów;
- zajęcia projektowe; w ramach tych zajęć student będzie wykonywał zadanie typu *studium na żywo* związane z zarządzaniem incydentami oraz prezentował na bieżąco wyniki i wnioski; Ponadto student będzie miał za zadanie wykonanie krytycznego przeglądu literatury naukowej, technicznej i biznesowej z zakresu cyberbezpieczeństwa;

Sprawdzanie założonych efektów kształcenia realizowane jest przez:
- ocenę wiedzy i umiejętności związanych z realizacją zadań laboratoryjnych – ocenę sprawozdań z realizacji zadań;
- ocenę wiedzy i umiejętności związanych z realizacją zadań projektowych – ocena prezentacji i raportu z przeglądu literatury;
- ocenę wiedzy i umiejętności wykazanych na sprawdzianie pisemnym o charakterze problemowym;

Wymiar w jednostkach ECTS: 5 pkt.

Liczba godzin pracy studenta związanych z osiągnięciem efektów kształcenia (opis):

1. liczba godzin kontaktowych – **62 godz**., w tym
   - obecność na wykładach: **30 godz.**,
   - obecność na zajęciach laboratoryjnych: **16 godz.**,
   - obecność na zajęciach projektowych: **4 godz.**,
   - udział w konsultacjach związanych z realizacją przedmiotu: **12 godz.**

2. praca własna studenta – **77 godz.**, w tym
   - analiza literatury i materiałów wykładowych związana z przygotowaniem do kolejnych wykładów: **10 godz.**
   - analiza literatury i materiałów wykładowych związana z przygotowaniem do laboratorium: **20 godz.**
   - realizacja projektu: **25 godz.** (studium na żywo) + **12 godz.** (analiza literatury i przygotowanie raportu) = **37 godz.**.
   - przygotowanie do kolokwium: **10 godz.**

Łączny nakład pracy studenta wynosi 139 godz., **co odpowiada** 5 pkt. **ECTS.**

Liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich: 2.25 pkt. ECTS, co odpowiada 62 godz. kontaktowym.

Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym: 3 pkt. ECTS co odpowiada 20+57 = 77 godz. realizacji projektu i laboratorium.

EFEKTY KSZTAŁCENIA/UCZENIA SIĘ

efekty kształcenia/uczenia się student, który zaliczył przedmiot:	**forma zajęć/ technika kształcenia**	**sposób weryfikacji (oceny)***	**odniesienie do efektów uczenia się dla programu**
WIEDZA			
w1: ma wiedzę dotyczącą fundamentalnych pojęć z zakresu cyberbezpieczeństwa	wykład + projekt + laboratorium	projekt, laboratorium, kololwium	W07 W09 W12
w2: ma wiedzę z zakresu mechanizmów stosowanych w złośliwym oprogramowaniu i sieciach botnet	wykład + projekt + laboratorium	laboratorium, kololwium	W07
w3: ma podstawową wiedzę z zakresu testów penetracyjnych	wykład + laboratorium	laboratorium kololwium	W07
w4: ma podstawową wiedzę z zakresu pozyskiwania i zabezpieczenia cyfrowego materiału dowodowego	wykład + laboratorium	laboratorium, kololwium	W07
w5: ma wiedzę z zakresu analizowania cyfrowego materiału dowodowego	wykład + laboratorium	laboratorium, kololwium	W07
w6: ma wiedzę metodyki procesu zarządzania incydentami	wykład + projekt	projekt, kololwium	W07
w7: ma podstawową wiedzę z obszaru środków technicznych zapewniających cyberbezpieczeństwo sieci, systemów i użytkowników	wykład + laboratorium + projekt	projekt, laboratorium, kololwium	W07
w8: ma podstawową wiedzę z zakresu modelowania zagrożeń	wykład + laboratorium + projekt	projekt, laboratorium, kololwium	W07 W12
UMIEJĘTNOŚCI			
u1: potrafi przygotować środowisko pracy pentestera	wykład + laboratorium	laboratorium	U03
u2: potrafi wykorzystywać podstawowe narzędzia do przeprowadzenia testów penetracyjnych	wykład + laboratorium	laboratorium	U03
u3: potrafi przeprowadzić podstawowy test penetracyjny zgodnie z przyjętą metodyką	wykład + laboratorium	laboratorium	U03
u4: potrafi stworzyć dokumentację z testów penetracyjnych zgodnie z przyjętą metodyką i wymaganiami	wykład + laboratorium	laboratorium	U03 U10
u5: potrafi zabezpieczyć cyfrowy materiał dowodowy z oprogramowania, systemów operacyjnych, serwerów i dysków	wykład + laboratorium	laboratorium	U08
u6: potrafi modelować zagrożenia zgodnie z metodyką Intrusion Kill Chain	wykład + projekt	projekt	U04 U07
u7: potrafi stosować środki techniczne zapewniające cyberbezpieczeństwo sieci, systemów i użytkowników	wykład + laboratorium	laboratorium	U08
u8: potrafi w podstawowym zakresie definiować procesy zarządzania incydentami naruszeń bezpieczeństwa sieci, systemów i użytkowników	wykład + laboratorium	laboratorium	U05 U07
u9: potrafi rozwiązywać zadania formułowane na bieżąco, komunikować wnioski i opinie, prowadzić na ich temat dyskusję i przekonywać innych	projekt	projekt	U09 U11
u10: potrafi przygotować i przeprowadzić prezentację dotyczącą określonego problemu z zakresu cyberbezpieczeństwa, z uwzględnieniem jego aspektów pozatechnicznych	projekt	projekt	U05 U10
u11: potrafi krytycznie analizować dostępną literaturę z zakresu domeny wiedzy	projekt	projekt	U01 U13
KOMPETENCJE SPOŁECZNE			
ks1: ma świadomość konieczności komunikowania się z otoczeniem, także pozazawodowym, w sposób zrozumiały dla odbiorcy	wykład + projekt + laboratorium	projekt + laboratorium	KS05
ks2: ma orientację zawodową w obszarze inżynierii cyberbepieczeństwa i jest świadomy procesu uczenia się w kierunku zwiększania kompetencji w tym obszarze	wykład + projekt	n/d	KS01

Wydziałowa Komisja Akredytacji Przedmiotów (WKAP)

Uwagi:

Data i podpis autora (kierownika zespołu autorskiego): później