"ZATWIERDZAM"

.....

.....

KARTA INFORMACYJNA PRZEDMIOTU

Nazwa przedmiotu	Inżynieria wsteczna złośliwego oprogramowania / Reverse engineering of malware
Kod przedmiotu	WCYKAWSM_REM
Język wykładowy	polski
Profil studiów	ogólnoakademicki
Forma studiów	studia stacjonarne
Poziom studiów	wojskowe studia jednolite magisterskie
Rodzaj przedmiotu	obowiązkowy
Obowiązuje od naboru	2021/2022

Forma zajęć, liczba godzin/rygor, razem godz., pkt ECTS

semestr	(x egzamin, + zaliczenie, # projekt)						punkty ECTS
	razem	wykłady	ćwiczenia	laboratoria	projekt	seminarium	
IX	44x	12		8+	24#		4.0
razem		12		8	24		4.0

Przedmioty wprowadzające	• Brak przedmiotów kształcenia wprowadzających
Semestr/kierunek studiów	semestr 9 / Kryptologia i cyberbezpieczeństwo / Bezpieczeństwo systemów informatycznych
Autor	dr inż. Jarosław Koszela
Jednostka odpowiedzialna za przedmiot	WCY/ISI
Skrócony opis przedmiotu	• Wykład - z wykorzystaniem klasycznych metody dydaktycznych (tablica, rzutnik, projektor) oraz praktycznym pokazem przykładowych rozwiązań i mechanizmów omawianych na wykładach. • Ćwiczenia laboratoryjne oraz realizacja projektu przejściowego - z wykorzystaniem środowiska i narzędzi do prowadzenia inżynierii wstecznej złośliwego oprogramowania (m. in. środowiska FLARE-VM oraz REMNUX).

Pełny opis przedmiotu (treści programowe)

lp.	Semestr IX temat/tematyka zajęć	liczba godzin wkł.	ćw.	lab.	prj.	sem.
1	Wprowadzenie tematyki inżynierii wstecznej implementacji programowych. Etapy procesu inżynierii wstecznej.	1				
2	Klasyfikacja zagrożeń. Obsługa incydentu. Aspekty prawne.	1			6	
3	Środowisko analityczne. Monitorowanie oprogramowania.	1		2		
4	Metody zabezpieczeń przed inżynierii wsteczną.	1			2	
5	Odwracanie skutków ataku. Słabości implementacji algorytmów kryptograficznych. Działania proaktywne. Zabezpieczenie materiału do analizy.	2		2	4	
6	Analiza statyczna.	2		1	4	
7	Analiza behawioralna.	2		1	4	
8	Analiza dynamiczna	2		2	4	
	Razem	12		8	24	

Literatura

podstawowa:
- P. Cichonski, T. Millar, T. Grance, K. Scarfone; Computer Security Incident Handling Guide; NIST Special Publication 800-61; 2015
- Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, Ph.D.; Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains; Lockheed Martin Corporation; 2011
- Intel® 64 and IA-32 Architectures Software Developer's Manual Volume 1: Basic Architecture; 2016

uzupełniająca:
- Ch. Eagle; IDA Pro Book. The Unofficial Guide to the World's Most Popular Disassembler; No Starch Press; 2011

Efekty uczenia się

Symbol	Efekty kształcenia	odniesienie do efektów kształcenia dla kierunku
W1	Zapoznać z metodami inżynierii wstecznej, metodami zabezpieczeń przed inżynierią wsteczną, klasyfikacją zagrożeń, obsługą incydentu, aspektami prawnymi.	K_W02, K_W05, K_U02, K_U05, K_U09
U1	Nauczyć konfigurować bezpieczne środowisko analityczne.	K_W02, K_W05, K_U02, K_U05, K_U09
U2	Nauczyć monitorować oprogramowanie.	K_W02, K_W05, K_U02, K_U05, K_U09
U3	Nauczyć zabezpieczać środowisko i doprowadzać do stanu sprzed incydentu	K_W02, K_W05, K_U02, K_U05, K_U09
U4	Nauczyć prowadzić analizę statyczną, behawioralną i dynamiczną oprogramowania złośliwego oraz wytwarzać ustrukturyzowaną	K_W02, K_W05, K_U02, K_U05, K_U09

	Symbol	Efekty kształcenia	odniesienie do efektów kształcenia dla kierunku
		informację zwrotną.	
Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez studenta zakładanych efektów uczenia się)	• Egzamin z przedmiotu jest realizowany na podstawie kolokwium egzaminacyjnego w formie pisemnej lub ustnej. Warunkiem dopuszczenia do egzaminu jest uzyskanie pozytywnej oceny z zaliczenia ćwiczeń laboratoryjnych i projektu przejściowego. W ocenie z egzaminu uwzględniona jest również ocen z ćwiczeń laboratoryjnych i projektu przejściowego. • Zaliczenie laboratorium i projektu: ocena wystawiona na podstawie wykonanego projektu z wykorzystaniem wybranych narzędzi do przeprowadzania inżynierii wstecznej oraz na podstawie sprawozdania z realizacji projektu przedstawionego w formie pisemnej i wygłoszonej prezentacji oraz ocen cząstkowych uzyskanych w trakcie zajęć laboratoryjnych		

Bilans ECTS (nakład pracy studenta)

SEMESTR 9		
Aktywność	**Obciążenie studenta**	
	Liczba godzin	**Liczba ECTS**
Udział w wykładach	12	0.5
Udział w laboratoriach	8	0.5
Udział w ćwiczeniach	0	0
Udział w projektach	24	1
Udział w seminariach	0	0
Samodzielne studiowanie tematyki wykładów	10	0.5
Samodzielne przygotowanie do laboratoriów	20	0.5
Samodzielne przygotowanie do ćwiczeń		
Samodzielna realizacja projektu	40	1
Samodzielne przygotowanie do seminariów		
Udział w konsultacjach		
Przygotowanie do egzaminu		
Przygotowanie do zaliczenia		
Udział w egzaminie / kolokwium	2	
Sumaryczne obciążenie pracą studenta	116	4
Zajęcia z udziałem nauczycieli	46	2
Zajęcia powiązane z działalnością naukową	114	4
Zajęcia o charakterze praktycznym	92	3

autor

dr inż. Jarosław Koszela
tytuł, stopień naukowy, imię, NAZWISKO, podpis

kierownik jednostki organizacyjnej odpowiedzialnej za przedmiot

dr hab. inż. Nowicki Tadeusz
tytuł, stopień naukowy, imię, NAZWISKO, podpis