SYLABUS PRZEDMIOTU

Inżynieria wsteczna złośliwego oprogramowania (Malware Reverse Engineering)

I. Informacje ogólne

Nazwa przedmiotu:	***Inżynieria wsteczna złośliwego programowania***
Kod przedmiotu:	IWZ
Rodzaj przedmiotu:	specjalistyczny
Kierunek studiów:	Informatyka
Poziom kształcenia:	II stopień
Profil kształcenia:	Ogólnoakademicki
Rok studiów:	drugi
Rodzaje zajęć i liczba godzin	
Wykład	0
Ćwiczenia	0
Laboratoria	30
Praktyki	0
Liczba punktów ECTS	3

Imię, nazwisko, tytuł/stopień naukowy, adres e-mail wykładowcy (wykładowców)/ prowadzących zajęcia

- mgr Maciej Krzyżaniak krzyzaniak.maciej@outlook.com

Język wykładowy	polski
Przedmiot prowadzony zdalnie (e-learning)	tak, częściowo

II. Informacje szczegółowe

1. Cele przedmiotu

Przedmiot stawia następujące cele:

- poznanie zasad działania oraz sposobów analizy złośliwego oprogramowania,

- nabycie umiejętności analizy plików binarnych,

- nabycie umiejętności analizy złośliwych skryptów,

- rozwój znajomości charakterystyki różnych protokołów sieciowych,

- poznanie zagrożeń, jakie stanowi złośliwe oporgramowanie dla przedsiębiorstw,

- rozwój znajomości zasad działania systemów operacyjnych.

2. Wymagania wstępne w zakresie wiedzy, umiejętności oraz kompetencji społecznych

Podstawowa wiedza z zakresu programowania.

Znajomość podstaw wirtualizacji.

Znajomość podstaw działania oraz umiejętność diagnozowania problemów systemów operacyjnych Windows oraz Linux.

3. Efekty uczenia się (EU) dla zajęć i odniesienie do efektów uczenia się (EK) dla kierunku studiów

Symbol EU dla przedmiotu	Symbol EK dla kierunku studiów	Po zakończeniu modułu i potwierdzeniu osiągnięcia EU student/ka:
IWZ_01	KINF2_U07 KINF2_K04	Potrafi wytłumaczyć, czym jest złośliwe oprogramowanie, przedstawić podstawowe techniki wykorzystywane do jego analizy.
IWZ_02	KINF2_U02 KINF2_U04 KINF2_U05 KINF2_U06 KINF2_U11	Potrafi stworzyć własne laboratorium do pracy ze złośliwym oprogramowaniem.
IWZ_03	KINF2_W03 KINF2_K02	Rozumie, czym są cechy statyczne plików, jak je sprawdzić i zinterpretować.

IWZ_04	KINF2_U02 KINF2_U04 KINF2_U05 KINF2_U06 KINF2_U11	Potrafi przeprowadzić analizę dynamiczną w bezpiecznym środowisku.
IWZ_05	KINF2_U02	Potrafi korzystać z debuggera.
IWZ_06	KINF2_U02	Zna popularne metody obfuskacji kodu.
IWZ_07	KINF2_W03 KINF2_W04 KINF2_K02	Wie, w jakim celu wykonuje się analizę złośliwego oprogramowania. Ma świadomość zagrożenia, jakie stanowi złośliwe oprogramowanie dla funkcjonowania społeczeństwa i gospodarki.
IWZ_08	KINF2_U02	Potrafi korzystać z deasemblera.
IWZ_09	KINF2_U02	Zna podstawy języka asembler.
IWZ_10	KINF2_U02 KINF2_U04 KINF2_U05 KINF2_U06 KINF2_U11	Potrafi przedstawić zasadę działania różnych typów złośliwego oprogramowania.
IWZ_11	KINF2_U02 KINF2_U04 KINF2_U05 KINF2_U06 KINF2_U11	Potrafi wykonać analizę ruchu sieciowego.
IWZ_12	KINF2_U02 KINF2_U05 KINF2_U06 KINF2_U11	Potrafi wykonać analizę złośliwych skryptów.
IWZ_13	KINF2_W03 KINF2_K02	Wie, z jakich technik utrudniających analizę korzystają twórcy złośliwego oprogramowania oraz jak je omijać.
IWZ_14	KINF2_U02	Potrafi wykonać analizę złośliwych dokumentów pakietu Microsoft Office oraz PDF.

IWZ_15	KINF2_U02	Potrafi przeprowadzić analizę zrzutu pamięci.

4. Treści programowe zapewniające uzyskanie efektów uczenia się (EU) z odniesieniem do odpowiednich efektów uczenia się (EU) dla przedmiotu

Lp.	Symbol EU dla przedmiotu	Godzin Wykład	Godzin ĆW/ LAB/ SEM	Godzin pracy własnej	Opis treści kształcenia modułu zajęć/przedmiotu
Suma		0	30	45	
1.	IWZ_01 IWZ_02		1	4	Wprowadzenie do analizy złośliwego oprogramowania: Czym jest złośliwe orpigramowanie?. Konfiguracja laboratorium do przeprowadzania analizy. Metody i techniki analizy.
2.	IWZ_03		3	4	Analiza statyczna: Narzędzia i techniki. *Open source intelligence*.
3.	IWZ_04		3	4	Analiza dynamiczna: Narzędzia i techniki monitorujące działanie złośliwego oprogramowania. Interakcja ze złośliwym oprogramowaniem.
4.	IWZ_05 IWZ_06		3	4	Podstawy analizy kodu: Korzystanie z debuggera. Popularne metody obfuskacji kodu.
5.	IWZ_07		1	0	Cele analizy: Cykl zapewniania bezpieczeństwa w przedsiębiorstwach. Rola analityków złośliwego oprogramowania. Indicators of Compromise (IOCs)
6.	IWZ_08 IWZ_09		4	4	Analiza kodu języka niskiego poziomu: Korzystanie z deasemblera. Podstawy języka asemblera.
7.	IWZ_10		4	6	Popularne techniki wykorzystywane przez złośliwe oprogramowanie: Rootkits. Keyloggers. Downloaders. HTTP C2 channels.
8.	IWZ_11		1	2	Przechwytywanie ruchu sieciowego: iNetSim, iptables, Wireshark.
9.	IWZ_12		2	3	Interakcja ze złośliwymi stronami internetowymi: tor, wget, curl, CapTipper, NetworkMiner. Deobfuskacja skryptów.
10.	IWZ_13		3	6	Self-defending malware: wykrywanie oraz omijanie zabezpieczeń utrudniających analizę.
11.	IWZ_14		3	4	Analiza złośliwych dokumentów: Pliki pakietu Microsoft Office. Pliki PDF.
12.	IWZ_15		2	4	Analiza pamięci. Czym jest i jakie korzyści daje analiza pamięci? Podstawy korzystania z pakietu Volatility.


Fundusze
Europejskie
Polska Cyfrowa
Rzeczpospolita
Polska
Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego

5. Zalecana literatura

1) Michael Sikorski, Andrew Honig, “Practical malware analysis : the hands-on guide to dissecting malicious software.”, No Starch Press, 2012
2) Gynvael Coldwind, Mateusz Jurczyk. “Praktyczna inżynieria wsteczna. Metody, techniki i narzędzia”, Wydawnictwo Naukowe PWN, 2016

V. Informacje dodatkowe

1. Metody i formy prowadzenia zajęć umożliwiające osiągnięcie założonych EU (proszę wskazać z proponowanych metod właściwe dla opisywanych zajęć lub/i zaproponować inne)

Realizacja	Metody i formy prowadzenia zajęć
✔	Wykład z prezentacją multimedialną wybranych zagadnień
	Wykład konwersatoryjny
	Wykład problemowy
	Dyskusja
	Praca z tekstem
✔	Metoda analizy przypadków
	Uczenie problemowe (Problem-based learning)
	Gra dydaktyczna/symulacyjna
	Rozwiązywanie zadań (np.: obliczeniowych, artystycznych, praktycznych)
	Metoda ćwiczeniowa
✔	Metoda laboratoryjna
	Metoda badawcza (dociekania naukowego)
	Metoda warsztatowa
	Metoda projektu
	Pokaz i obserwacja
	Demonstracje dźwiękowe i/lub video
	Metody aktywizujące (np.: „burza mózgów”, technika analizy SWOT, technika drzewka decyzyjnego, metoda „kuli śniegowej”, konstruowanie „map myśli”)
	Praca w grupach

✔	Wykład zdalny w czasie rzeczywistym
	Wykład zdalny asynchroniczny uzupełniony spotkaniem w czasie rzeczywistym
	Wykład zdalny asynchroniczny z aktywnością studenta uzupełniony spotkaniem w czasie rzeczywistym
✔	Ćwiczenia/laboratoria/konwersatoria zdalne w czasie rzeczywistym
	Ćwiczenia zdalne asynchroniczne z pracą indywidualną studenta uzupełnione spotkaniem w czasie rzeczywistym
	Ćwiczenia zdalne asynchroniczne z pracą grupową studentów uzupełnione spotkaniem w czasie rzeczywistym
	Laboratorium cyfrowe zdalne uzupełnione spotkaniem w czasie rzeczywistym
	Konwersatorium asynchroniczne zdalne uzupełnione spotkaniem w czasie rzeczywistym
	Seminarium zdalne w czasie rzeczywistym
	Seminarium asynchroniczne zdalne ze spotkaniem w czasie rzeczywistym
	Inne (jakie?) -

2. Sposoby oceniania stopnia osiągnięcia EU (proszę wskazać z proponowanych sposobów właściwe dla danego EU lub/i zaproponować inne

	Symbole EU dla modułu zajęć/przedmiotu

Sposoby oceniania

	IWZ : 01, 02, 03, 04, 05, 06, 07, 08, 09, 10, 11, 12. 13, 14, 15									
Egzamin pisemny										
Egzamin ustny										
Egzamin z „otwartą książką”										
Kolokwium pisemne										
Kolokwium ustne										
Test										
Projekt										
Esej										
Raport	✔									
Prezentacja multimedialna										
Egzamin praktyczny (obserwacja wykonawstwa)	✔									
Portfolio										
Zadania cząstkowe na wykładzie										

Zadania cząstkowe na laboratoriach	✔									

3. Nakład pracy studenta i punkty ECTS

Forma aktywności		Średnia liczba godzin na zrealizowanie aktywności
Godziny zajęć (wg planu studiów) z nauczycielem		30
Praca własna studenta*	Przygotowanie do zajęć	20
	Czytanie wskazanej literatury	10
	Przygotowanie pracy pisemnej, raportu, prezentacji, itp.	0
	Przygotowanie projektu	0
	Przygotowanie pracy semestralnej	0
	Przygotowanie do egzaminu/zaliczenia	0
	Praca z materiałem do samokształcenia (np. Jupyter Notebook)	15
	Praca z laboratorium cyfrowym (np. Code Runner)	30
	Inne (jakie?)	
SUMA GODZIN		75
LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU		3

* proszę wskazać z proponowanych przykładów pracy własnej studenta właściwe dla opisywanego modułu lub/i zaproponować inne

4. Kryteria oceniania wg skali stosowanej w UAM

Ocena	Kryterium
bardzo dobry (bdb; 5,0)	od 85% punktów
dobry plus (+db; 4,5)	od 75% punktów
dobry (db; 4,0)	od 65% punktów
dostateczny plus (+dst; 3,5)	od 55% punktów
dostateczny (dst; 3,0)	od 50% punktów

niedostateczny (ndst; 2,0)	poniżej 50% punktów