Inżynieria wsteczna złośliwego oprogramowania

Sylabus zajęć

Informacje podstawowe

Kierunek studiów Informatyka **Specjalność** - **Jednostka organizacyjna** Wydział Matematyki i Informatyki **Poziom studiów** studia drugiego stopnia poinżynierskie **Forma studiów** studia stacjonarne **Profil studiów** profil ogólnoakademicki	**Cykl dydaktyczny** 2024/25 **Kod zajęć** 06INFS.42S.01032.24 **Języki wykładowe** polski **Obligatoryjność** Fakultatywny **Blok zajęciowy** Przedmioty specjalnościowe

Koordynator zajęć	Tomasz Kowalski
Prowadzący zajęcia	Michał Krzyżaniak

Okres	**Forma zajęć / liczba godzin / forma zaliczenia**	**Liczba punktów ECTS**
Semestr 2	• Laboratorium: 30, Zaliczenie z oceną	3

Cele kształcenia dla zajęć

Kod	Cel
C1	Poznanie zasad działania oraz sposobów analizy złośliwego oprogramowania.
C2	Nabycie umiejętności analizy plików binarnych.
C3	Nabycie umiejętności analizy złośliwych skryptów.
C4	Rozwój znajomości charakterystyki różnych protokołów sieciowych.
C5	Poznanie zagrożeń, jakie stanowi złośliwe oprogramowanie dla przedsiębiorstw - rozwój znajomości zasad działania systemów operacyjnych.

Wymagania wstępne

Podstawowa wiedza z zakresu programowania. Znajomość podstaw wirtualizacji. Znajomość podstaw działania oraz umiejętność diagnozowania problemów systemów operacyjnych Windows oraz Linux.

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			
W1	Rozumie, czym są cechy statyczne plików, jak je sprawdzić i zinterpretować.	INF_K4_W03	Raport, Egzamin praktyczny (obserwacja wykonawstwa) oraz zadania wykonywane podczas zajęć
W2	Zna popularne metody obfuskacji kodu.	INF_K4_W03	Raport, Egzamin praktyczny (obserwacja wykonawstwa) oraz zadania wykonywane podczas zajęć
W3	Wie, w jakim celu wykonuje się analizę złośliwego oprogramowania. Ma świadomość zagrożenia, jakie stanowi złośliwe oprogramowanie dla funkcjonowania społeczeństwa i gospodarki.	INF_K4_W03, INF_K4_W04	Raport, Egzamin praktyczny (obserwacja wykonawstwa) oraz zadania wykonywane podczas zajęć
W4	Wie, z jakich technik utrudniających analizę korzystają twórcy złośliwego oprogramowania oraz jak je omijać.	INF_K4_W03	Raport, Egzamin praktyczny (obserwacja wykonawstwa) oraz zadania wykonywane podczas zajęć
Umiejętności – Student/ka:			
U1	Potrafi wytłumaczyć, czym jest złośliwe oprogramowanie, przedstawić podstawowe techniki wykorzystywane do jego analizy.	INF_K4_U07	Raport, Egzamin praktyczny (obserwacja wykonawstwa) oraz zadania wykonywane podczas zajęć
U2	Potrafi stworzyć własne laboratorium do pracy ze złośliwym oprogramowaniem.	INF_K4_U02, INF_K4_U04, INF_K4_U05, INF_K4_U06, INF_K4_U11	Raport, Egzamin praktyczny (obserwacja wykonawstwa) oraz zadania wykonywane podczas zajęć
U3	Potrafi przeprowadzić analizę dynamiczną w bezpiecznym środowisku.	INF_K4_U02, INF_K4_U04, INF_K4_U05, INF_K4_U06, INF_K4_U11	Raport, Egzamin praktyczny (obserwacja wykonawstwa) oraz zadania wykonywane podczas zajęć
U4	Potrafi korzystać z debuggera.	INF_K4_U02	Raport, Egzamin praktyczny (obserwacja wykonawstwa) oraz zadania wykonywane podczas zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
U5	Potrafi korzystać z deasemblera.	INF_K4_U02	Raport, Egzamin praktyczny (obserwacja wykonawstwa) oraz zadania wykonywane podczas zajęć
U6	Zna podstawy języka asembler.	INF_K4_U02	Raport, Egzamin praktyczny (obserwacja wykonawstwa) oraz zadania wykonywane podczas zajęć
U7	Potrafi przedstawić zasadę działania różnych typów złośliwego oprogramowania.	INF_K4_U02, INF_K4_U04, INF_K4_U05, INF_K4_U06, INF_K4_U11	Raport, Egzamin praktyczny (obserwacja wykonawstwa) oraz zadania wykonywane podczas zajęć
U8	Potrafi wykonać analizę ruchu sieciowego.	INF_K4_U02, INF_K4_U04, INF_K4_U05, INF_K4_U06, INF_K4_U11	Raport, Egzamin praktyczny (obserwacja wykonawstwa) oraz zadania wykonywane podczas zajęć
U9	Potrafi wykonać analizę złośliwych skryptów.	INF_K4_U02, INF_K4_U05, INF_K4_U06, INF_K4_U11	Raport, Egzamin praktyczny (obserwacja wykonawstwa) oraz zadania wykonywane podczas zajęć
U10	Potrafi wykonać analizę złośliwych dokumentów pakietu Microsoft Office oraz PDF.	INF_K4_U02	Raport, Egzamin praktyczny (obserwacja wykonawstwa) oraz zadania wykonywane podczas zajęć
U11	Potrafi przeprowadzić analizę zrzutu pamięci.	INF_K4_U02	Raport, Egzamin praktyczny (obserwacja wykonawstwa) oraz zadania wykonywane podczas zajęć

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Wprowadzenie do analizy złośliwego oprogramowania: Czym jest złośliwe orpigramowanie?. Konfiguracja laboratorium do przeprowadzania analizy. Metody i techniki analizy.	U1, U2	Laboratorium
2.	Analiza statyczna: Narzędzia i techniki. Open source intelligence.	W1	Laboratorium
3.	Analiza dynamiczna: Narzędzia i techniki monitorujące działanie złośliwego oprogramowania. Interakcja ze złośliwym oprogramowaniem.	U3	Laboratorium
4.	Podstawy analizy kodu: Korzystanie z debuggera. Popularne metody obfuskacji kodu.	W2, U4	Laboratorium

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
5.	Cele analizy: Cykl zapewniania bezpieczeństwa w przedsiębiorstwach. Rola analityków złośliwego oprogramowania. Indicators of Compromise (IOCs)	W3	Laboratorium
6.	Analiza kodu języka niskiego poziomu: Korzystanie z deasemblera. Podstawy języka asemblera.	U5, U6	Laboratorium
7.	Popularne techniki wykorzystywane przez złośliwe oprogramowanie: Rootkits. Keyloggers. Downloaders. HTTP C2 channels.	U7	Laboratorium
8.	Przechwytywanie ruchu sieciowego: iNetSim, iptables, Wireshark.	U8	Laboratorium
9.	Interakcja ze złośliwymi stronami internetowymi: tor, wget, curl, CapTipper, NetworkMiner. Deobfuskacja skryptów.	U9	Laboratorium
10.	Self-defending malware: wykrywanie oraz omijanie zabezpieczeń utrudniających analizę.	W4	Laboratorium
11.	Analiza złośliwych dokumentów: Pliki pakietu Microsoft Office. Pliki PDF.	U10	Laboratorium
12.	Analiza pamięci. Czym jest i jakie korzyści daje analiza pamięci? Podstawy korzystania z pakietu Volatility.	U11	Laboratorium

Informacje dodatkowe

Forma zajęć	Metody i formy prowadzenia zajęć
Laboratorium	Wykład z prezentacją multimedialną wybranych zagadnień, Metoda analizy przypadków, Metoda laboratoryjna

Forma zajęć	Warunki zaliczenia zajęć
Laboratorium	Końcowa ocena składa się z następujących elementów: 1. raport – 33.3%, 2. egzamin praktyczny – 33.4%, 3. zadania wykonywane podczas zajęć – 33.3%. Skala ocen: 1. bardzo dobry (bdb; 5,0) – od 85% punktów, 2. dobry plus (db plus; 4,5) – od 75% punktów, 3. dobry (db; 4,0) – od 65% punktów, 4. dostateczny plus (dst plus; 3,5) – od 55% punktów, 5. dostateczny (dst; 3,0) – od 50% punktów, 6. niedostateczny (ndst; 2,0) – poniżej 50% punktów.

Literatura

Obowiązkowa

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

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	**Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć**
Laboratorium	30
Przygotowanie do zajęć	10
Czytanie wskazanej literatury	5
Przygotowanie raportu	5
Inne	25
Łączny nakład pracy studenta	**Liczba godzin** 75
Liczba punktów ECTS	**ECTS** 3

* godzina (lekcyjna) oznacza 45 minut

Efekty uczenia się dla kierunku

Kod	Treść
INF_K4_U02	Absolwent/ka potrafi adaptować istniejące oraz tworzyć nowe metody informatyczne do rozwiązywania nieszablonowych problemów praktycznych i teoretycznych
INF_K4_U04	Absolwent/ka potrafi projektować i implementować systemy informatyczne o różnej złożoności i różnych architekturach
INF_K4_U05	Absolwent/ka potrafi formułować i testować nowe algorytmy i metody rozwiązywania problemów w wybranych obszarach informatyki na potrzeby prowadzenia prac badawczo-rozwojowych z uwzględnieniem aktualnego stanu wiedzy
INF_K4_U06	Absolwent/ka potrafi rozwiązywać złożone problemy z wybranych obszarów informatyki oraz proponować nowe algorytmy, narzędzia i metody wykorzystując odpowiednio dobrane źródła, które poddaje krytycznej analizie, syntezie i twórczej interpretacji
INF_K4_U07	Absolwent/ka potrafi wyrażać krytyczne opinie na temat architektury oraz użyteczności wykorzystywanych systemów informatycznych
INF_K4_U11	Absolwent/ka potrafi pozyskiwać informacje z literatury, baz wiedzy, Internetu oraz innych wiarygodnych źródeł, integrować je, dokonywać ich interpretacji oraz wyciągać wnioski i formułować opinie
INF_K4_W03	Absolwent/ka zna i rozumie w pogłębionym stopniu współczesne metody, narzędzia i technologie informatyczne właściwe dla wybranych obszarów zastosowań niezbędne przy budowie złożonych systemów informatycznych oraz przy prowadzeniu prac badawczo-rozwojowych
INF_K4_W04	Absolwent/ka zna i rozumie zasady rozwiązywania problemów z wykorzystaniem zaawansowanych algorytmów i metod informatycznych