SYLABUS PRZEDMIOTU

Wykrywanie ataków sieciowych

I. Informacje ogólne

Nazwa przedmiotu	*Wykrywanie ataków sieciowych*
Kod przedmiotu	WAS
Rodzaj przedmiotu	specjalistyczny
Kierunek studiów	Informatyka
Poziom kształcenia	II stopień
Profil kształcenia	Ogólnoakademicki
Rok studiów	drugi
Rodzaje zajęć i liczba godzin	
Wykład	30
Ćwiczenia	
Laboratoria	30
Praktyki	0
Liczba punktów ECTS	6

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

- Dr inż. Marcin Gogolewski marcing@amu.edu.pl

Język wykładowy	polski
Przedmiot prowadzony zdalnie (e-learning)	nie (choć możliwy b-learning)

II. Informacje szczegółowe

1. Cele przedmiotu

Przedmiot stawia następujące cele:

- podniesienie poziomu świadomości nt. bezpieczeństwa sieci i problemów z tym związanych
- nauka stosowania narzędzi informatycznych wspomagających wykrywanie i przeciwdziałanie atakom sieciowym

- poznanie wybranych niskopoziomowych algorytmów i mechanizmów wspomagających wydajne analizy ruchu sieciowego
- nauka pisania reguł dla systemów wykrywania włamań

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

Umiejętność programowania na poziomie inżyniera informatyki.
Podstawy sieci komputerowych na poziomie inżyniera informatyki.
Język angielski w stopniu umożliwiającym biegłe posługiwanie się dokumentacją.

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:
WAS_01	KINF2-W03, KINF2-U04	Zna w pogłębionym stopniu problematykę sieci komputerowych.
WAS_02	KINF2_U12	Potrafi przygotować złożony warsztat pracy z wykorzystaniem maszyn wirtualnych i dostępnego oprogramowania.
WAS_03	KINF2_W02	Potrafi rozróżniać różne typy pasywnych zabezpieczeń sieciowych i zna podstawy konfiguracji sieci.
WAS_04	KINF2_W02	Zna problematykę zabezpieczeń aktywnych.
WAS_05	KINF2_W03	Rozumie podstawowe zasady działania protokołów HTTP, SPDY oraz QUIC. Rozumie problemy związane z wydajnym wykorzystaniem sieci komputerowych do udostępniania treści.
WAS_06	KINF2_U04, KINF2_U07	Rozumie idee i sposoby zabezpieczeń serwerów http. Potrafi analizować logi bezpieczeństwa wybranego serwera.
WAS_07	KINF2_U11	Potrafi przeprowadzić rozpoznanie sieci z wykorzystaniem zarówno narzędzi kontaktowych, jak i bezkontaktowych.
WAS_08	KINF2_W03, KINF2_U06	Zna zaawansowane aspekty konfiguracji systemów IPS.

WAS_09	KINF2_W03, KINF2_U02	Zna i potrafi stosować wybrane oprogramowanie do przeprowadzania testów penetracyjnych.
WAS_10	KINF2_U11	Zna wybrane, zaawansowane metody pozyskiwania wiedzy o atakach sieciowych
WAS_11	KINF2_U11, KINF2_U12	Zna podział i powody ataków na systemy komputerowe.
WAS_12	KINF2_W03	Zna narzędzia wyszukiwania błędów w oprogramowaniu.
WAS_13	KINF2_U02	Zna narzędzia i potrafi tworzyć reguły wybranych narzędzi ochrony antywirusowej i analizy plików.
WAS_14	KINF2_U02	Zna narzędzia i potrafi tworzyć reguły wybranych narzędzi ochrony antyspamowej.
WAS_15	KINF2_U06	Potrafi pisać reguły systemów wykrywania i przeciwdziałania atakom.
WAS_16	KINF2_W03	Zna i rozumie wybrane parametry sprzętu i systemu operacyjnego, istotne w procesie wydajnego wykrywania zagrożeń.
WAS_17	KINF2_W02	Zna wybrane narzędzia służące do *phishingu* i ochrony przed *phishingiem*, rozumie ich działanie i ograniczenia.
WAS_18	KINF2_W02	Zna i rozumie problem podszywania się w sieci.
WAS_19	KINF2_W01	Zna i rozumie miary skuteczności systemów oraz granice ich wydajności.

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		30	30	90	
1.	WAS_01	2		6	Krótkie wprowadzenie do sieci komputerowych, protokół TCP/IPv4 i TCP/IPv6 (TCP/UDP/ICMP). Przypomnienie i uszczegółowienie wiedzy zdobytej na studiach inżynierskich.
2.	WAS_02		3	4	Przygotowanie środowiska pracy, instalacja oprogramowania na maszynach wirtualnych
3.	WAS_03	1	1	4	Zapory sieciowe, serwery *proxy* (rodzaje, funkcjonalność, zasady działania i możliwości), lokalizacja sensorów (problemy), ukrywanie zabezpieczeń
4.	WAS_04	1	1	2	Systemy pasywne i aktywne (IDS, IPS), przykładowe systemy (*Snort – Cisco, Suricata* i inne), programy „antywirusowe" (wprowadzenie), wymagania dla systemów IPS
5.	WAS_05	2	2	2	Protokół http – problemy z protokołem, nowe pomysły (SPDY, QUIC), wpływ na bezpieczeństwo
6.	WAS_06	1	2	3	Zabezpieczanie serwerów HTTP (reguły *ModSecurity*, czytanie logów)
7.	WAS_07	2	2	5	Metody skanowania sieci (narzędzia bezkontaktowe i kontaktowe)
8.	WAS_08	3	4	8	Konfiguracja *Snort/Suricata*, preprocesory, interpretacja wyników programów
9.	WAS_09	3	4	9	Narzędzia do przeprowadzania testów penetracyjnych, etapy ataku, narzędzia, wykorzystanie *Metasploita*, przykładowe ataki
10.	WAS_10	2		1	Sposoby pozyskiwania danych o atakach (*honypots*, podejrzane zachowania, anomalie), sygnatury ataków
11.	WAS_11	2		2	Podstawowe powody włamań i naruszeń bezpieczeństwa

12.	WAS_12	4	3	6	Wykrywanie problemów w oprogramowaniu (podstawy np. *Valgrinda*), zabezpieczenia sprzętowe systemów operacyjnych
13.	WAS_13	1	1	2	Narzędzia analizy przesyłanych danych (np. program *ClamAV* i połączenie go z IPS, pisanie reguł do *ClamAV*), *Safe Browsing*.
14.	WAS_14	1	1	2	Narzędzia wykrywania i analizy SPAMu, techniki
15.	WAS_15	2	2	4	Pisanie reguł systemów IPS, dodatkowe źródła reguł
16.	WAS_16	1	1	2	Techniczne aspekty wykrywania ataków (ustawienia systemu operacyjnego, kart sieciowych, przechwytywania pakietów), Algorytmy wyszukiwania wzorców (w łańcuchach).
17.	WAS_17	1	1	2	Ataki *phishingowe* (narzędzia do organizacji ataków i sposoby wykrywania)
18.	WAS_18	1	1	2	*Spoofing*, projekty typu *HoneyPot*, skanowanie portów i ochrona
19.	WAS_19	1	1	2	Miary skuteczności systemów wykrywających ataki, próby wykrywania ataków metodami sztucznej inteligencji, ograniczenia systemów wykrywania

5. Zalecana literatura

1) Bartosz Danowski, Łukasz Kozicki, Spam. Profilaktyka i obrona, Helion, 2004
2) Michael Rash, Jake Babbin, Becky Pinkard, Graham Clark, Angela Orebaugh, „IPS zapobieganie i aktywne przeciwdziałanie intruzom", Mikom 2005
3) Georgia Weidman, „Penetration Testing: A Hands-on Introduction to Hacking", no starch press, 2014
4) Jaswal Nipun, „Mastering Metasploit", Packt Publishing Limited, 2016
5) David Kennedy , Jim O'Gorman (Author), Devon Kearns, Mati Aharoni, „Metasploit: The Penetration Tester's Guide", 2014
6) Alex Lukatsky, Wykrywanie włamań i aktywna ochrona danych, Helion, 2004

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

	WAS: 01.03-06.10-12, 15, 17	WAS: 02-10, 12-18								
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										
…										

3. Nakład pracy studenta i punkty ECTS

Forma aktywności		Średnia liczba godzin na zrealizowanie aktywności
Godziny zajęć (wg planu studiów) z nauczycielem		60
Praca własna studenta*	Przygotowanie do zajęć	10
	Czytanie wskazanej literatury	5
	Przygotowanie pracy pisemnej, raportu, prezentacji, itp.	
	Przygotowanie prac domowych	53
	Przygotowanie pracy semestralnej	0
	Przygotowanie do egzaminu/zaliczenia	15
	Praca z materiałem do samokształcenia (np. Jupyter Notebook)	0
	Praca z laboratorium cyfrowym (np. Code Runner)	0
	Inne (jakie?) - konfiguracja sprzętu, instalacja i konfiguracja oprogramowania	7
SUMA GODZIN		150
LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU		6

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

4. Kryteria oceniania wg skali stosowanej w UAM – zaliczenie (bez punktów za egzamin, maksymalnie 70%)

Ocena	Kryterium
bardzo dobry (bdb; 5,0)	od 64% punktów
dobry plus (+db; 4,5)	od 57% punktów
dobry (db; 4,0)	od 50% punktów
dostateczny plus (+dst; 3,5)	od 43% punktów
dostateczny (dst; 3,0)	od 36% punktów

niedostateczny (ndst; 2,0)	poniżej 36% punktów

5. Kryteria oceniania wg skali stosowanej w UAM – wykład (suma wszystkich punktów)

Ocena	Kryterium
bardzo dobry (bdb; 5,0)	od 91% punktów
dobry plus (+db; 4,5)	od 81% punktów
dobry (db; 4,0)	od 71% punktów
dostateczny plus (+dst; 3,5)	od 61% punktów
dostateczny (dst; 3,0)	od 51% punktów
niedostateczny (ndst; 2,0)	poniżej 51% punktów