

"ZATWIERDZAM"**KARTA INFORMACYJNA PRZEDMIOTU**

Nazwa przedmiotu	Ataki sieciowe i złośliwe oprogramowanie					Cyber Attacks and Malware				
Kod przedmiotu	WCYIRWSM_.....									
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			
	VI	44+	10		20+	14+		5.0		
	razem		10		20	14		5.0		
Przedmioty wprowadzające	● Brak przedmiotów kształcenia wprowadzających									
Semestr/kierunek studiów	semestr 6 / Informatyka / Systemy teleinformatyczne - bezpieczeństwo systemów teleinformatycznych									
Autor	dr inż. Adam Patkowski									
Jednostka odpowiedzialna za przedmiot	Wydział Cybernetyki/Instytut Teleinformatyki i Cyberbezpieczeństwa/ZSK									
Skrócony opis przedmiotu	● Wykłady przy komputerze ● Ćwiczenia laboratoryjne									
Pełny opis przedmiotu (treści programowe)	lp.	Semestr VI temat/tematyka zajęć				liczba godzin				
						wkł.	ćw.	lab.	prj.	sem.
	1	Wprowadzenie do malware. Klasyfikacja.				4				
	2	Ataki lokalne. Narzędzia i techniki śledcze. Badanie malware. Zasady bezpieczeństwa.				2		2		
	3	Hooks. Przepełnienia bufora i sterty, Shellcodes.				2		2		
	4	Znane payloads, ich ukrywanie (obfuscation) i wykorzystanie jako RATs. Kali Linux.						4		
	5	Ataki w sieciach lokalnych i ataki zdalne. Narzędzia. Exploitation tools.						4		
	6	Ataki złożone.				2		8		
	7	Opracowanie i prezentacja wskazanej techniki ataku.							14	
	Razem				10		20	14		
Literatura	podstawowa:									
	● Kali Linux (aktualny stan projektu i powiązanych wg http://kali.org) ● MITRE ATT&CK (aktualny stan wg http://attack.mitre.org) ● NIST: National Vulnerability Database (aktualny stan wg http://nvd.nist.gov) ● Rapid7: Metasploit (aktualny stan projektu wg https://www.metasploit.com/) ● Farbianiec D.: Techniki twórców złośliwego oprogramowania. Elementarz programisty. Helion 2014. ● Gregg Michael: Certified Ethical Hacker Exam Prep. Que Publishing 2006. ● Monika Agarwal, Abhinav Singh: Metasploit. Receptury pentestera. Wydanie II. Helion 2014. ● Offensive Security: exploit-db.com uzupełniająca: ● Aktualne materiały z Internetu (hackme, CTF, tutorials) ● Dokumentacje z: Intel® 64 and IA-32 Architectures Software Developer Manuals AMD Developer Central: Developer Guides, Manuals & ISA Documents ● Joseph Muniz, Aamir Lakhani: Kali Linux. Testy penetracyjne. ● Hyde Randall: Art of Assembly Language Programming ● Shellcodes database for study cases (http://shell-storm.org/shellcode/) ● Ben Clark: Red Team Field Manual.									
Efekty uczenia się	Symbol	Efekty kształcenia					odniesienie do efektów kształcenia dla kierunku			
	W13	Znajomość rodzajów i zasad działania malware.					K_U12, K_W14			
	U2	Umiejętność wykrywania malware i bezpiecznego ich badania.					K_U12, K_W14			
	W46	Znajomość podstawowych rodzajów cyberataków					K_U12, K_W14			
	U4	Umiejętność uzupełniania wiedzy o nowych exploitach, payloads i możliwościach ich wykorzystania					K_U12, K_W14			
	U56	Umiejętność wykorzystywania dostępnych narzędzi cyberataków					K_U12, K_W14			

	Symbol	Efekty kształcenia	odniesienie do efektów kształcenia dla kierunku	
		(w tym także social engineering, malware i RATs) i rozpoznawania sposobu ich działania		
Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez studenta zakładanych efektów uczenia się)	• Przedmiot zaliczany jest na podstawie ocen z laboratoriów (60%) i projektu (40%). Obie oceny muszą być pozytywne. • Laboratorium zaliczane jest na podstawie ocen bieżących z wykonywania ćwiczeń oraz kolokwium. Do zaliczenia wymagana jest obecność na 80% zajęć laboratoryjnych. • Projekt zaliczany jest na podstawie pisemnego sprawozdania z postawionego zadania. Projekt może być realizowany indywidualnie lub przez grupę studentów. Ocena jest wystawiana przez prowadzącego na podstawie sprawozdania i prezentacji wyniku. • Ćwiczenia laboratoryjne uczą i weryfikują efekty U2, U4 i U56. Projekt ugruntowuje umiejętności nabyte na ćwiczeniach laboratoryjnych, w szczególności U4, pozwala także zweryfikować efekty W13 i U46.			
Bilans ECTS (nakład pracy studenta)	SEMESTR 6			
	Aktywność	Obciążenie studenta		
		Liczba godzin	Liczba ECTS	
	Udział w wykładach	10	1	
	Udział w laboratoriach	20	2	
	Udział w ćwiczeniach	0	0	
	Udział w projektach	14	0	
	Udział w seminariach	0	0	
	Samodzielne studiowanie tematyki wykładów	24		
	Samodzielne przygotowanie do laboratoriów	16		
	Samodzielne przygotowanie do ćwiczeń			
	Samodzielna realizacja projektu	48	2	
	Samodzielne przygotowanie do seminariów			
	Udział w konsultacjach			
	Przygotowanie do egzaminu			
	Przygotowanie do zaliczenia			
	Udział w egzaminie / kolokwium			
	Sumaryczne obciążenie pracą studenta	132	5	
	Zajęcia z udziałem nauczycieli	44	3	
	Zajęcia powiązane z działalnością naukową	132	5	
	Zajęcia o charakterze praktycznym	98	4	

autor

**kierownik jednostki organizacyjnej
odpowiedzialnej za przedmiot**

dr inż. Adam Patkowski

tytuł, stopień naukowy, imię, NAZWISKO, podpis

dr inż. Malinowski Tomasz

tytuł, stopień naukowy, imię, NAZWISKO, podpis