"ZATWIERDZAM"

.....

.....

KARTA INFORMACYJNA PRZEDMIOTU

Nazwa przedmiotu	Eksploracja sieci teleinformatycznych	Exploration of ICT networks
Kod przedmiotu	WCYKCWSM_.....	
Język wykładowy	polski	
Profil studiów	ogólnoakademicki	
Forma studiów	studia stacjonarne	
Poziom studiów	wojskowe studia jednolite magisterskie	
Rodzaj przedmiotu		
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	44x	14		20+	10#		4.0
razem		14		20	10		4.0

Przedmioty wprowadzające	• Sieci komputerowe - • Systemy operacyjne -
Semestr/kierunek studiów	semestr 6 / Kryptologia i cyberbezpieczeństwo / Cyberobrona
Autor	dr inż. Tomasz Malinowski, mgr inż. Michał Jarosz
Jednostka odpowiedzialna za przedmiot	Wydział Cybernetyki / Instytut Teleinformatyki i Cyberbezpieczeństwa / Zakład Bezpieczeństwa Teleinformatycznego
Skrócony opis przedmiotu	• Wykłady przeprowadzane z wykorzystaniem środków audiowizualnych jako elementów wspomagających. • Samodzielne studiowanie zaleconej literatury. • Ćwiczenia laboratoryjne polegające na samodzielnym realizowaniu czynności związanych z wyszukiwaniem informacji o zasobach systemów teleinformatycznych oraz opracowywanie sprawozdań ze zrealizowanych ćwiczeń laboratoryjnych. • Bieżące sprawdzanie zakresu opanowania fragmentów materiału niezbędnego do poprawnego wykonania ćwiczeń laboratoryjnych, realizowane w formie sprawdzianów wstępnych (tzw. wejściówek). • Samodzielne realizowanie projektów dotyczących wybranej fazy eksploracji systemu teleinformatycznego. • Końcowe sprawdzenie zakresu opanowania materiału, realizowane w formie egzaminu.

Pełny opis przedmiotu (treści programowe)

lp.	Semestr VI temat/tematyka zajęć	liczba godzin				
		wkł.	ćw.	lab.	prj.	sem.
1	Wstęp.	2				
2	Rekonesans aktywny i pasywny.	4			10	
3	Identyfikacja podatności.	1		4		
4	Skanowanie hostów i portów.	3		4		
5	Identyfikacja systemów operacyjnych (fingerprinting).	2		4		
6	Enumeracja kont, zasobów i aplikacji.	2		8		
	Razem	14		20	10	

Literatura

podstawowa:

- Scambray J., McClure S., Kurtz G., Hacking Exposed 7, McGrow Hill 2012 (tłumacz. Hacking zdemaskowany, PWN 2005 - wydanie 5).
- Allen L., Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide, Packt Publishing Ltd, 2012
- Suski Z., Wybrane przypadki enumeracji systemu Windows Server 2012, Przegląd Teleinformatyczny 1-2/ 2014, Instytut Teleinformatyki i Automatyki, Warszawa 2014.
- Suski Z., Rekonesans pasywny w testach penetracyjnych, Przegląd Teleinformatyczny 3-4/2017, Instytut Teleinformatyki i Automatyki, Warszawa 2017.
- Pillay R., Learn Penetration Testing Packt Publishing Ltd, 2019.
- Suski Z., Techniki skanowania. Rozdz. 10 w monografii Bezpieczeństwo teleinformatyczne - problemy formalne i techniczne, WAT 2006.

uzupełniająca:

- Wilhelm T., Professional Penetration Testing - Creating and Operating a Formal Hacking Lab, Syngress Elsevier, 2013.
- Engebretson P., The Basics of Hacking and Penetration, Syngress Elsevier, 2013.
- McClure S., Scambray J., Hacking Exposed Windows 3rd Edition-Windows Security Secrets and Solutions, Mc Graw Hill, 2008.
- Whitaker A., Newman D., P., Penetration Testing and Network Defense, Cisco Press, 2006.
- Allen L., Heriyanto T., Ali S., Kali Linux - Assuring Security by Penetration Testing, Packt Publishing Ltd, 2014
- Pale P., C., Nmap 6: Network Exploration and Security Auditing Cookbook, Packt Publishing Ltd, 2012.
- Materiały udostępnione przez prowadzącego zajęcia.

	• Materiały internetowe.

Efekty uczenia się

Symbol	Efekty kształcenia	odniesienie do efektów kształcenia dla kierunku
W1	Ma wiedzę w zakresie wybranych faktów, obiektów i zjawisk oraz dotyczących ich metod i teorii w obszarze bezpieczeństwa systemów teleinformatycznych.	K_W14
W2	Ma wiedzę w zakresie metodologii badań oraz praktycznych przykładów implementacji metod stosowanych do rozwiązywania typowych problemów w obszarze bezpieczeństwa systemów teleinformatycznych.	K_W14
U1	Umie formułować, analizować i znajdować rozwiązania problemów w obszarze bezpieczeństwa systemów teleinformatycznych. Potrafi planować i przeprowadzać eksperymenty w obszarze bezpieczeństwa systemów teleinformatycznych, interpretować ich wyniki i wyciągać wnioski.	K_U11

Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez studenta zakładanych efektów uczenia się)

- Przedmiot zaliczany jest na podstawie egzaminu. Egzamin jest przeprowadzany w formie testu wyboru.
- Warunkiem dopuszczenia do egzaminu jest zaliczenie ćwiczeń laboratoryjnych i projektu oraz przedstawienie dokumentów określonych w regulaminie studiów.
- Warunkiem koniecznym zaliczenia egzaminu jest uzyskanie z testu przynajmniej 50% możliwych do zdobycia punktów. Punkty są przeliczane na ocenę według takiej samej zasady jak w przypadku ćwiczeń laboratoryjnych.
- Zaliczenie ćwiczeń laboratoryjnych odbywa się na podstawie sumy punktów uzyskanych za realizację zadań bieżących (ocenianych na podstawie sprawozdań) i sprawdziany bieżące ("wejściówki").
- Nie będą przyjmowane sprawozdania od osób, które nie uczestniczyły w zajęciach laboratoryjnych.
- Punkty są przeliczane na ocenę według zasady: ocena 5 - co najmniej 90% punktów ocena 4,5 - co najmniej 80% punktów ocena 4 - co najmniej 70% punktów ocena 3,5 - co najmniej 60% punktów ocena 3 - co najmniej 50% punktów ocena 2 - poniżej 50% punktów.
- Ocena zaliczeniowa projektu wynika z jakości wykonania zadania (również sprawozdania) oraz terminu jego oddania: - Zadania oddane zadania w terminie podstawowym są oceniane przy zastosowaniu pełnej skali ocen. - Za zadania oddane zadania w terminie sesji poprawkowej można uzyskać co najwyżej ocenę dobrą. - Za zadania oddane zadania w terminie dodatkowym można uzyskać co najwyżej ocenę dostateczną.
- Efekty W1 i W2 sprawdzane są za pomocą testu egzaminacyjnego i sprawdzianów bieżących.
- Efekt U1 sprawdzany jest za pomocą sprawozdań z ćwiczeń laboratoryjnych i projektu.

Bilans ECTS (nakład pracy studenta)

SEMESTR 6

Aktywność	Obciążenie studenta	
	Liczba godzin	Liczba ECTS
Udział w wykładach	14	0.25
Udział w laboratoriach	20	0.75
Udział w ćwiczeniach	0	0
Udział w projektach	10	0.1
Udział w seminariach	0	0
Samodzielne studiowanie tematyki wykładów	5	0.15
Samodzielne przygotowanie do laboratoriów	25	1
Samodzielne przygotowanie do ćwiczeń		
Samodzielna realizacja projektu	50	1
Samodzielne przygotowanie do seminariów		
Udział w konsultacjach		
Przygotowanie do egzaminu	15	0.75
Przygotowanie do zaliczenia		
Udział w egzaminie / kolokwium		
Sumaryczne obciążenie pracą studenta	139	4
Zajęcia z udziałem nauczycieli	44	1.1
Zajęcia powiązane z działalnością naukową	124	3.25
Zajęcia o charakterze praktycznym	105	2.85

autorzy

dr inż. Tomasz Malinowski
tytuł, stopień naukowy, imię, NAZWISKO, podpis

mgr inż. Michał Jarosz
tytuł, stopień naukowy, imię, NAZWISKO, podpis

kierownik jednostki organizacyjnej odpowiedzialnej za przedmiot

dr inż. Malinowski Tomasz
tytuł, stopień naukowy, imię, NAZWISKO, podpis