SYLABUS PRZEDMIOTU

Testy Penetracyjne

I. Informacje ogólne

Nazwa przedmiotu:	*Testy penetracyjne*
Kod przedmiotu:	TEP
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
Praktyk i	0
Liczba punktów ECTS	3

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

- mgr inż. Piotr Kaźmierczak piotr.kazmierczak@pm.me

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

II. Informacje szczegółowe

1. Cele przedmiotu

Przedmiot stawia następujące cele:

- zapoznanie z metodykami prowadzenia testów penetracyjnych

- zbudowanie solidnych podstaw i nawyków przydatnych podczas wykonywania testów penetracyjnych

- pobudzenie kreatywności i niekonwencjonalnego myślenia niezbędnego w pracy testera penetracyjnego

- zapoznanie z technikami białego wywiadu w celu pasywnego pozyskiwania danych o celu

- zapoznania z technikami aktywnego pozyskiwania informacji w sieciach i systemach opartych o systemy Linux jak i Windows

- zbudowanie solidnych podstaw w tematyce prowadzenia testów penetracyjnych aplikacji webowych

- przedstawienie dodatkowych zagadnień (jak ataki socjotechniczne czy ataki na sieci-wifi) przydatnych podczas testów penetracyjnych

- zbudowanie umiejętności prawidłowego raportowania wyników testu penetracyjnego

- wskazanie możliwych specjalizacji i kierunków samorozwoju.

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

Znajomość budowy i funkcjonowania sieci TCP/IP w szczególności protokołów TCP/UDP oraz protokołów aplikacyjnych http(s), DNS, FTEP, telnet, SSH, SMB.

Podstawowa umiejętność administracji systemami Linux i Windows.

Podstawowe umiejętności z zakresu programowania skryptowego.

Znajomość funkcjonowania aplikacji webowych oraz baz danych.

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:
TEP_01	KINF2_W06	Rozumie etyczne oraz prawne obostrzenia dotyczące testów penetracyjnych.
TEP_02	KINF2_U05 KINF2_U06 KINF2_U07 KINF2_U11	Potrafi zainicjować test penetracyjny oraz przygotować niezbędne środowisko pracy.
TEP_03	KINF2_U05 KINF2_U06 KINF2_U07 KINF2_U10 KINF2_U11	Potrafi przygotować prawidłowy raport z testu penetracyjnego.
TEP_04	KINF2_U05 KINF2_U06 KINF2_U07 KINF2_U11	Potrafi przeprowadzić rekonesans pasywny na temat sieci/domeny/firmy będącej celem testu penetracyjnego.
TEP_05	KINF2_U05 KINF2_U06 KINF2_U07 KINF2_U11	Potrafi przeprowadzić rekonesans aktywny na temat sieci/systemu będącego celem testu penetracyjnego.
TEP_06	KINF2_U05 KINF2_U06 KINF2_U07 KINF2_U11	Potrafi zaprogramować proste narzędzia automatyzujące pracę podczas testu penetracyjnego.
TEP_07	KINF2_U05 KINF2_U06 KINF2_U07 KINF2_U11	Potrafi przeprowadzić enumerację systemu Linux.
TEP_08	KINF2_U05 KINF2_U06 KINF2_U07 KINF2_U11	Potrafi przeprowadzić enumerację systemu Windows.
TEP_09	KINF2_W02 KINF2_W03 KINF2_W04 KINF2_W05	Zna zagadnienia związane z podnoszeniem uprawnień.

	KINF2_W06	
TEP_10	KINF2_U05 KINF2_U06 KINF2_U07 KINF2_U11	Potrafi korzystać ze skanera podatności oraz interpretować wyniki skanów.
TEP_11	KINF2_U05 KINF2_U06 KINF2_U07 KINF2_U11	Potrafi wyszukiwać podatności na podstawie zdobytych informacji.
TEP_12	KINF2_U05 KINF2_U06 KINF2_U07 KINF2_U11	Zna aspekty pracy z *exploitami* oraz potrafi z nich skorzystać.
TEP_13	KINF2_U05 KINF2_U06 KINF2_U07 KINF2_U11	Potrafi przeprowadzić zdalny atak na systemy uwierzytelniające różnych usług.
TEP_14	KINF2_U05 KINF2_U06 KINF2_U07 KINF2_U11	Potrafi przeprowadzić atak offline na różnego rodzaju skróty haseł.
TEP_15	KINF2_W02 KINF2_W03 KINF2_W04 KINF2_W05 KINF2_W06	Zna metodykę prowadzenia testu penetracyjnego aplikacji webowej.
TEP_16	KINF2_U05 KINF2_U06 KINF2_U07 KINF2_U11	Potrafi mapować aplikację webową oraz wykrywać ukryte zasoby.
TEP_17	KINF2_U05 KINF2_U06 KINF2_U07 KINF2_U11	Potrafi namierzyć i wykorzystać podstawowe błędy obsługi danych od użytkownika.
TEP_18	KINF2_U05 KINF2_U06 KINF2_U07 KINF2_U11	Potrafi namierzyć i wykorzystać podatności związane z obsługą plików.
TEP_19	KINF2_U05 KINF2_U06 KINF2_U07 KINF2_U11	Potrafi namierzyć i wykorzystać inne podatności w aplikacjach webowych.

TEP_20	KINF2_W02 KINF2_W03 KINF2_W04 KINF2_W05 KINF2_W06	Zna techniki *postexploitacyjne* w systemach Linux i Windows.
TEP_21	KINF2_U05 KINF2_U06 KINF2_U07 KINF2_U11	Potrafi wykorzystać oprogramowanie *metasploit framework* podczas testu penetracyjnego.
TEP_22	KINF2_U05 KINF2_U06 KINF2_U07 KINF2_U11	Zna zasadę działania ataków typu *client-side*.
TEP_23	KINF2_U05 KINF2_U06 KINF2_U07 KINF2_U11 KINF2_K04 KINF2_K06	Zna metodykę ataków socjotechnicznych oraz potrafi przeprowadzić symulację ataku *phishingowego*.
TEP_24	KINF2_W02 KINF2_W03 KINF2_W04 KINF2_W05 KINF2_W06	Zna podstawowe techniki omijania mechanizmów bezpieczeństwa.
TEP_25	KINF2_U05 KINF2_U06 KINF2_U07 KINF2_U11	Potrafi przełamać zabezpieczenia sieci-wifi opartej o WPA2.

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.	TEP_01 TEP_02		2	2	**Wprowadzenie do testów penetracyjnych:** Metodyki prowadzenia testów penetracyjnych. Zapoznanie z etycznymi oraz prawnymi aspektami testów penetracyjnych. Wskazanie kierunków rozwoju, źródeł i sposobów nabywania umiejętności oraz omówienie przydatnej literatury. Przygotowanie środowiska laboratoryjnego.
2	TEP_03		1	1	**Raportowanie testu penetracyjnego:** Przygotowanie szablonu raportu z testu penetracyjnego. Omówienie istotnych elementów raportu oraz kryteriów świadczących o jego jakości. Otwarcie raportu z opisem przeprowadzonych działań w trakcie trwania kursu, który będzie głównym elementem zaliczenia kursu.
3.	TEP_04		2	2	**Rekonesans pasywny:** Omówienie metod przeprowadzania białego wywiadu, informacji jakie mogą być przydatne do dalszych działań oraz przedstawienie publicznie dostępnych źródeł.
4.	TEP_05		2	2	**Rekonesans aktywny:** Wprowadzenie do aktywnej enumeracji sieci wraz z przedstawieniem niezbędnika narzędziowego każdego *pentestera*.
5.	TEP_06		1	2	**Programowanie:** Automatyzacja prac wykonywanych przez *pentestera* z wykorzystaniem języków programowania i poleceń powłoki (*Python, Bash, Powershell*).
6.	TEP_07 TEP_09		1	3	**Enumeracja w systemach Linux:** Przeprowadzenie rekonesansu w systemie Linux. Wykorzystanie błędów konfiguracji systemu i działającym na nich usług do podniesienia uprawnień oraz pozyskania informacji użytecznych podczas testu penetracyjnego.
7.	TEP_08 TEP_09		1	3	**Enumeracja w systemach Windows:** Przeprowadzenie rekonesansu w systemie Windows. Wykorzystanie błędów konfiguracji systemu i działającym na nich usług do podniesienia uprawnień oraz pozyskania

					informacji użytecznych podczas testu penetracyjnego.
8.	TEP_10 TEP_11 TEP_12		2	2	**Ocena podatności:** Analiza zdobytych informacji, metody wyszukiwania podatności. Wykorzystanie skanerów podatności. Praca z *exploitami*.
9.	TEP_13 TEP_14		1	1	**Ataki na hasła:** Przeprowadzenie ataków na zdalne mechanizmy uwierzytelniające. Przeprowadzenie ataków offline na różnego rodzaju skróty haseł.
10.	TEP_15 TEP_16		3	4	**Testy penetracyjne aplikacji webowych:** Metodyka prowadzenia testów penetracyjnych aplikacji webowych. Modelowanie zagrożeń. Przydatne narzędzia. Zdobywanie informacji o celu. Mapowanie aplikacji. Wykrywanie ukrytych zasobów.
11.	TEP_17		2	4	**Podstawowe błędy obsługi danych od użytkownika:** Wykrywanie i wykorzystywanie podatności typu *SQL Injection, Cross-Site Scripting, Code Injection*.
12.	TEP_18		2	4	**Podatności związane z obsługą plików:** Wykrywanie podatności typu *Local/Remote File Inclusion*. Wykrywanie podatności związanych z uploadem plików oraz obsługą różnych rozszerzeń (XML, SVG).
13.	TEP_19		2	4	**Pozostałe podatności w aplikacjach webowych:** Ataki na mechanizmy zarządzania sesją, wykorzystanie podatności *Cross-Site Request Forgery*, analiza podatności w logice biznesowej aplikacji, wykorzystanie podatności typu *Server Side Request Forgery*. Wykorzystanie podatności związanych z deserializacją danych.
14.	TEP_20		2	3	**Techniki postexploitacyjne w systemach Linux i Windows:** Alternatywne sposoby transferu plików. Podnoszenie uprawnień w systemie. *Lateral movements*. Przekierowania portów i tunelowanie ruchu.
15.	TEP_21		2	2	**Metasploit framework:** Praca z narzędziem *msfconsole*. Wykorzystanie narzędzia *meterpreter*. Omówienie dodatkowych narzędzi z pakietu *msf*.
16.	TEP_22 TEP_23		1	2	**Ataki typu client-side:** Opracowanie ataku typu *client-side*. Wprowadzenie do ataków socjotechnicznych i przeprowadzenie ataku phishingowego.
17.	TEP_24		1	2	**Techniki omijania:** Omówienie zasad funkcjonowania mechanizmów bezpieczeństwa typu anty wirus, *web application firewall* czy filtr

					antyspamowy. Przeprowadzenie działań mających na celu ich ominięcie.
18.	TEP_25		1	2	**Sieci Wi-Fi:** Omówienie sposobów ataków na sieci wi-fi oraz ich klientów. Przeprowadzenie ataku na standard WPA2.
19.			1	0	**Podsumowanie kursu:** Prezentacja stworzonych raportów oraz ich omówienie.

5. Zalecana literatura

1) Dafydd Stuttard, Marcus Pinto, „The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws 2nd Edition", Wiley, 2011
2) Peter Kim, "The Hacker Playbook 3: Practical Guide To Penetration Testing", Independently published, 2018
3) Jon Erickson, "Hacking: The Art of Exploitation, 2nd Edition", No Starch Press, 2008
4) Thomas Wilhelm, "Professional Penetration Testing: Creating and Learning in a Hacking Lab 2nd Edition", Syngress, 2013
5) Michał Bentkowski, Artur Czyż, Rafał Janicki, Jarosław Kamiński, Adrian Michalczyk, Mateusz Niezabitowski, Marcin Piosek, Michał Sajdak, Grzegorz Trawiński, Bohdan Widła, „Bezpieczeńswo aplikacji webowych", Securitum Szkolenia, 2019
6) Stuart McClure, Joel Scambray, George Kurtz, "Hacking Exposed 7: Network Security Secrets and Solutions 7th Edition", McGraw-Hill Education 2012
7) The Open Source Security Testing Methodology Manual, https://www.isecom.org/OSSTMM.3.pdf, (data odczytu treści: 09.11.2020)
8) Standard PTES, http://www.pentest-standard.org/index.php/Main_Page, (data odczytu treści: 09.11.2020)
9) OWASP Testing Guide v4.1, https://owasp.org/www-project-web-security-testing-guide/v41/ (data odczytu treści: 09.11.2020)
10) OWASP Application Security Verification Standard v4.0.2, https://raw.githubusercontent.com/OWASP/ASVS/v4.0.2/4.0/OWASP%20Application%20Security%20Verification%20Standard%204.0.2-en.pdf (data odczytu treści: 09.11.2020)

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

	TEP: 01, 02, 10, 12, 22, 25	TEP: 03, 04, 05, 07, 08, 09, 11, 13, 14, 15, 16, 17, 18, 19, 20, 21	TEP: 06, 13, 14, 15, 23, 24							
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 laboratorium			✔							

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	5
	Czytanie wskazanej literatury	5
	Przygotowanie pracy pisemnej, raportu, prezentacji, itp.	10
	Przygotowanie projektu	0
	Przygotowanie pracy semestralnej	0
	Przygotowanie do egzaminu/zaliczenia	0
	Praca z materiałem do samokształcenia (np. Jupyter Notebook)	5
	Praca z laboratorium cyfrowym (np. Code Runner)	20
	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 88% punktów
dobry plus (+db; 4,5)	od 80% punktów
dobry (db; 4,0)	od 70% punktów
dostateczny plus (+dst; 3,5)	od 60% punktów
dostateczny (dst; 3,0)	od 50% punktów
niedostateczny (ndst; 2,0)	poniżej 50% punktów