UNIWERSYTET IM. ADAMA MICKIEWICZA W POZNANIU

Testy penetracyjne

Sylabus zajęć

Informacje podstawowe

Kierunek studiów Informatyka **Specjalność** - **Jednostka organizacyjna** Wydział Matematyki i Informatyki **Poziom studiów** studia drugiego stopnia poinżynierskie **Forma studiów** studia niestacjonarne **Profil studiów** profil ogólnoakademicki	**Cykl dydaktyczny** 2023/24 **Kod zajęć** 06INFN.41S.01012.23 **Języki wykładowe** polski **Obligatoryjność** Fakultatywny **Blok zajęciowy** Przedmioty specjalnościowe

Koordynator zajęć	Piotr Kaźmierczak
Prowadzący zajęcia	Piotr Kaźmierczak

Okres	**Forma zajęć / liczba godzin / forma zaliczenia**	**Liczba punktów ECTS**
Semestr 1	• Laboratorium: 15, Zaliczenie z oceną	3

Cele kształcenia dla zajęć

Kod	Cel
C1	Zapoznanie z metodykami prowadzenia testów penetracyjnych.
C2	Zbudowanie solidnych podstaw i nawyków przydatnych podczas wykonywania testów penetracyjnych.
C3	Pobudzenie kreatywności i niekonwencjonalnego myślenia niezbędnego w pracy testera penetracyjnego.
C4	Zapoznanie z technikami białego wywiadu w celu pasywnego pozyskiwania danych o celu.
C5	Zapoznania z technikami aktywnego pozyskiwania informacji w sieciach i systemach opartych o systemy Linux jak i Windows.
C6	Zbudowanie solidnych podstaw w tematyce prowadzenia testów penetracyjnych aplikacji webowych.
C7	Przedstawienie dodatkowych zagadnień (jak ataki socjotechniczne czy ataki na sieci WiFi) przydatnych podczas testów penetracyjnych.
C8	Zbudowanie umiejętności prawidłowego raportowania wyników testu penetracyjnego.
C9	Wskazanie możliwych specjalizacji i kierunków samorozwoju.

Wymagania wstępne

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.

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 etyczne oraz prawne obostrzenia dotyczące testów penetracyjnych.	INF_K4_W06	Egzamin praktyczny (obserwacja wykonawstwa) oraz zadania wykonywane podczas zajęć
W2	Zna metodykę prowadzenia testu penetracyjnego aplikacji webowej.	INF_K4_W02, INF_K4_W03, INF_K4_W04, INF_K4_W05, INF_K4_W06	Raport, Egzamin praktyczny (obserwacja wykonawstwa) oraz zadania wykonywane podczas zajęć
W3	Zna techniki postexploitacyjne w systemach Linux i Windows.	INF_K4_W02, INF_K4_W03, INF_K4_W04	Raport
W4	Zna podstawowe techniki omijania mechanizmów bezpieczeństwa.	INF_K4_W02, INF_K4_W03, INF_K4_W04, INF_K4_W05, INF_K4_W06	Egzamin praktyczny (obserwacja wykonawstwa) oraz zadania wykonywane podczas zajęć
Umiejętności – Student/ka:			

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
U1	Potrafi zainicjować test penetracyjny oraz przygotować niezbędne środowisko pracy.	INF_K4_U05, INF_K4_U06, INF_K4_U07, INF_K4_U11	Egzamin praktyczny (obserwacja wykonawstwa) oraz zadania wykonywane podczas zajęć
U2	Potrafi przygotować prawidłowy raport z testu penetracyjnego.	INF_K4_U05, INF_K4_U06, INF_K4_U07, INF_K4_U10, INF_K4_U11	Raport
U3	Potrafi przeprowadzić rekonesans pasywny na temat sieci/domeny/firmy będącej celem testu penetracyjnego.	INF_K4_U05, INF_K4_U06, INF_K4_U07, INF_K4_U11	Raport
U4	Potrafi przeprowadzić rekonesans aktywny na temat sieci/systemu będącego celem testu penetracyjnego.	INF_K4_U05, INF_K4_U06, INF_K4_U07, INF_K4_U11	Raport
U5	Potrafi zaprogramować proste narzędzia automatyzujące pracę podczas testu penetracyjnego.	INF_K4_U05, INF_K4_U06, INF_K4_U07, INF_K4_U11	Egzamin praktyczny (obserwacja wykonawstwa) oraz zadania wykonywane podczas zajęć
U6	Potrafi przeprowadzić enumerację systemu Linux.	INF_K4_U05, INF_K4_U06, INF_K4_U07, INF_K4_U11	Raport
U7	Potrafi przeprowadzić enumerację systemu Windows.	INF_K4_U05, INF_K4_U06, INF_K4_U07, INF_K4_U11	Raport
U8	Potrafi wykorzystać w praktyce zagadnienia związane z podnoszeniem uprawnień.	INF_K4_U05, INF_K4_U06, INF_K4_U07, INF_K4_U11	Raport
U9	Potrafi korzystać ze skanera podatności oraz interpretować wyniki skanów.	INF_K4_U05, INF_K4_U06, INF_K4_U07, INF_K4_U11	Egzamin praktyczny (obserwacja wykonawstwa) oraz zadania wykonywane podczas zajęć
U10	Potrafi wyszukiwać podatności na podstawie zdobytych informacji.	INF_K4_U05, INF_K4_U06, INF_K4_U07, INF_K4_U11	Raport
U11	Zna aspekty pracy z exploitami oraz potrafi z nich skorzystać.	INF_K4_U05, INF_K4_U06, INF_K4_U07, INF_K4_U11	Egzamin praktyczny (obserwacja wykonawstwa) oraz zadania wykonywane podczas zajęć
U12	Potrafi przeprowadzić zdalny atak na systemy uwierzytelniające różnych usług.	INF_K4_U05, INF_K4_U06, INF_K4_U07, INF_K4_U11	Egzamin praktyczny (obserwacja wykonawstwa) oraz zadania wykonywane podczas zajęć
U13	Potrafi przeprowadzić atak offline na różnego rodzaju skróty haseł.	INF_K4_U05, INF_K4_U06, INF_K4_U07, INF_K4_U11	Raport, Egzamin praktyczny (obserwacja wykonawstwa) oraz zadania wykonywane podczas zajęć
U14	Potrafi mapować aplikację webową oraz wykrywać ukryte zasoby.	INF_K4_U05, INF_K4_U06, INF_K4_U07, INF_K4_U11	Raport
U15	Potrafi namierzyć i wykorzystać podstawowe błędy obsługi danych od użytkownika.	INF_K4_U05, INF_K4_U06, INF_K4_U07, INF_K4_U11	Raport

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
U16	Potrafi namierzyć i wykorzystać podatności związane z obsługą plików	INF_K4_U05, INF_K4_U06, INF_K4_U07, INF_K4_U11	Raport
U17	Potrafi namierzyć i wykorzystać inne podatności w aplikacjach webowych.	INF_K4_U05, INF_K4_U06, INF_K4_U07, INF_K4_U11	Raport
U18	Potrafi wykorzystać oprogramowanie podczas testu penetracyjnego.	INF_K4_U05, INF_K4_U06, INF_K4_U07, INF_K4_U11	Raport
U19	Zna zasadę działania ataków typu client-side.	INF_K4_U05, INF_K4_U06, INF_K4_U07, INF_K4_U11	Egzamin praktyczny (obserwacja wykonawstwa) oraz zadania wykonywane podczas zajęć
U20	Potrafi przeprowadzić symulację ataku phishingowego.	INF_K4_U05, INF_K4_U06, INF_K4_U07, INF_K4_U11	Egzamin praktyczny (obserwacja wykonawstwa) oraz zadania wykonywane podczas zajęć
U21	Potrafi przełamać zabezpieczenia sieci-wifi opartej o WPA2.	INF_K4_U05, INF_K4_U06, INF_K4_U07, INF_K4_U11	Egzamin praktyczny (obserwacja wykonawstwa) oraz zadania wykonywane podczas zajęć
Kompetencji społecznych – Student/ka:			
K1	Zna metodykę ataków socjotechnicznych.	INF_K4_K04, INF_K4_K06	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 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.	W1, U1	Laboratorium
2.	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.	U2	Laboratorium
3.	Rekonesans pasywny: Omówienie metod przeprowadzania białego wywiadu, informacji jakie mogą być przydatne do dalszych działań oraz przedstawienie publicznie dostępnych źródeł.	U3	Laboratorium

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
4.	Rekonesans aktywny: Wprowadzenie do aktywnej enumeracji sieci wraz z przedstawieniem niezbędnika narzędziowego każdego pentestera.	U4	Laboratorium
5.	Programowanie: Automatyzacja prac wykonywanych przez pentestera z wykorzystaniem języków programowania i poleceń powłoki (Python, Bash, Powershell).	U5	Laboratorium
6.	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.	U6, U8	Laboratorium
7.	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.	U7, U8	Laboratorium
8.	Ocena podatności: Analiza zdobytych informacji, metody wyszukiwania podatności. Wykorzystanie skanerów podatności. Praca z exploitami.	U10, U11, U9	Laboratorium
9.	Ataki na hasła: Przeprowadzenie ataków na zdalne mechanizmy uwierzytelniające. Przeprowadzenie ataków offline na różnego rodzaju skróty haseł.	U12, U13	Laboratorium
10.	Testy penetracyjne aplikacji webowych: Metodyka prowadzenia testów penetracyjnych aplikacji webowych. Modelowanie zagrożeń. Przydatne narzędzia. Zdobywanie informacji o celu. Mapowanie aplikacji. Wykrywanie ukrytych zasobów.	W2, U14	Laboratorium
11.	Podstawowe błędy obsługi danych od użytkownika: Wykrywanie i wykorzystywanie podatności typu SQL Injection, Cross-Site Scripting, Code Injection.	U15	Laboratorium
12.	Podatności związane z obsługą plików: Wykrywanie podatności typu Local/Remote File Inclusion. Wykrywanie podatności związanych z uploadem plików oraz obsługą różnych rozszerzeń (XML, SVG).	U16	Laboratorium
13.	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.	U17	Laboratorium
14.	Techniki postexploitacyjne w systemach Linux i Windows: Alternatywne sposoby transferu plików. Podnoszenie uprawnień w systemie. Lateral movements. Przekierowania portów i tunelowanie ruchu.	W3	Laboratorium
15.	Metasploit framework: Praca z narzędziem msfconsole. Wykorzystanie narzędzia meterpreter. Omówienie dodatkowych narzędzi z pakietu msf.	U18	Laboratorium
16.	Ataki typu client-side: Opracowanie ataku typu client-side. Wprowadzenie do ataków socjotechnicznych i przeprowadzenie ataku phishingowego.	U19, U20, K1	Laboratorium

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
17.	Techniki omijania: Omówienie zasad funkcjonowania mechanizmów bezpieczeństwa typu anty wirus, web application firewall czy filtr antyspamowy. Przeprowadzenie działań mających na celu ich ominięcie.	W4	Laboratorium
18.	Sieci Wi-Fi: Omówienie sposobów ataków na sieci wi-fi oraz ich klientów. Przeprowadzenie ataku na standard WPA2.	U21	Laboratorium

Informacje dodatkowe

Forma zajęć	Metody i formy prowadzenia zajęć
Laboratorium	Metoda analizy przypadków, Uczenie problemowe (Problem-based learning), Gra dydaktyczna/symulacyjna, Rozwiązywanie zadań (np.: obliczeniowych, artystycznych, praktycznych), Metoda laboratoryjna, Metoda projektu, Pokaz i obserwacja, Praca w grupach

Forma zajęć	Warunki zaliczenia zajęć
Laboratorium	Końcowa ocena składa się z następujących elementów: 1. raport – 1/3 punktów, 2. egzamin praktyczny (obserwacja wykonawstwa) – 1/3 punktów, 3. zadania wykonywane podczas zajęć – 1/3 punktów. Skala ocen: 1. bardzo dobry (bdb; 5,0) – od 88% punktów, 2. dobry plus (db plus; 4,5) – od 80% punktów, 3. dobry (db; 4,0) – od 70% punktów, 4. dostateczny plus (dst plus; 3,5) – od 60% punktów, 5. dostateczny (dst; 3,0) – od 50% punktów, 6. niedostateczny (ndst; 2,0) – poniżej 50% punktów.

Literatura

Obowiązkowa

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-securitytesting-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%20A pplication%20Security%20Verification%20Standard%204.0.2-en.pdf (data odczytu treści: 09.11.2020)

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	**Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć**
Laboratorium	15
Przygotowanie do zajęć	20
Czytanie wskazanej literatury	5
Przygotowanie raportu	10
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_K04	Absolwent/ka jest gotów/gotowa do rozpoznania najważniejszych osiągnięć w swojej dziedzinie i stojących przed nią wyzwań; potrafi je przedstawić laikom w sposób popularny
INF_K4_K06	Absolwent/ka jest gotów/gotowa do pogłębiania świadomości roli informatyki w kształtowaniu życia społecznego
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_U10	Absolwent/ka potrafi przygotować obszerne dokumentacje, opracowania i raporty w języku polskim i języku obcym, w tym z wykorzystaniem ujęć teoretycznych, a także różnych źródeł
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_W02	Absolwent/ka zna i rozumie współczesny stan badań i tendencje rozwojowe w wiodących obszarach informatyki
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
INF_K4_W05	Absolwent/ka zna i rozumie budowę oraz cykl życia przykładowych systemów informatycznych wykorzystywanych w praktyce oraz zna ograniczenia złożonych systemów informatycznych
INF_K4_W06	Absolwent/ka zna i rozumie zagadnienia prawne i społeczne aspekty informatyki, w tym odpowiedzialności zawodowej i etycznej, kodeksów etycznych, własności intelektualnej, prywatności i swobód obywatelskich, ryzyka i odpowiedzialności związanej z systemami informatycznymi