KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Testy penetracyjne [S1Cybez1>TP]

Przedmiot

Kierunek studiów
Cyberbezpieczeństwo

Rok/Semestr
3/5

Studia w zakresie (specjalność)
–

Profil studiów
ogólnoakademicki

Poziom studiów
pierwszego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obligatoryjny

Liczba godzin

Wykład
8

Laboratorium
24

Inne
0

Ćwiczenia
0

Projekty/seminaria
0

Liczba punktów ECTS

2,00

Koordynatorzy

dr hab. inż. Sławomir Hanczewski
slawomir.hanczewski@put.poznan.pl

Wykładowcy

Wymagania wstępne

Student ma uporządkowaną i podbudowaną teoretycznie wiedzę w zakresie działania sieci teleinformatycznych w tym protokołów sieciowych i usług oferowanych w tych sieciach. Student potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie. Student potrafi pracować indywidualnie i w zespole. Student ma świadomość ważności i rozumie pozatechniczne aspekty i skutki działalności inżyniera- specjalisty w zakresie cyberbezpieczeństwa i związaną z tym odpowiedzialność za podejmowane decyzje. Powinien również rozumieć konieczność poszerzania swoich kompetencji. Ponadto w zakresie kompetencji społecznych student musi prezentować takie postawy jak uczciwość, odpowiedzialność, wytrwałość, ciekawość poznawcza, kreatywność, kultura osobista, szacunek dla innych ludzi.

Cel przedmiotu

Przedstawienie teoretycznych i praktycznych zagadnień związanych z testami penetracyjnymi sieci komputerowych.

Przedmiotowe efekty uczenia się

Wiedza:
Student ma zaawansowaną i szczegółową wiedzę z zakresu szeroko rozumianych testów penetracyjnych sieci komputerowych. Wiedza obejmuje: 1. zasady testów penetracyjnych, 2. planowanie i przeprowadzanie testów (wewnętrznych i zewnętrznych), 3. dokumentacja potestowa. [K1_W10]
Student posiada wiedzę o trendach rozwoju testów penetracyjnych. [K1_W20]

Umiejętności:
Student potrafi pozyskiwać informacje o testach penetracyjnych i sieciach komputerowych z literatury, baz danych oraz innych źródeł (w języku polskim i angielskim). [K1_U01]
Student potrafi również integrować wiedzę na temat testów penetracyjnych oraz potrafi ocenić przydatność metod i narzędzi do przygotowania i przeprowadzenia testów. [K1_U06]
Potrafi też współdziałać w zespole, przyjmując w nim różne role i wyznaczać kierunki dalszej nauki. [K1_U15]

Kompetencje społeczne:
Student rozumie, że w zakresie sieci komputerowych i testów penetracyjnych wiedza i umiejętności szybko się dezaktualizują. [K1_K01]
Rozumie również, jak ważne jest korzystanie z najnowszej wiedzy. [K1_K02]

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:
Wiedza zdobyta na wykładach weryfikowana za pomoca testu. Test składa się z 30 pytań , na które proponuje się 4 odpowiedzi, ale tylko jedna odpowiedź jest prawidłowa. Zagadnienia końcowe, na podstawie których przygotowywane są pytania, zostaną rozesłane do studentów pocztą elektroniczną z wykorzystaniem uczelnianego systemu poczty elektronicznej.
Wiedza i umiejętności nabyte podczas ćwiczeń laboratoryjnych są weryfikowane na bierząco przez prowadzącegoe zajęcia. Brak zaliczenia ćwiczenia powoduje konieczność powtórzenia go w wyznaczonym przez prowadzącego terminie.
W każdej formie zaliczenia przedmiotu ocena zależy od liczby zdobytych przez studenta punktów w stosunku do maksymalnej liczby punktów obowiązkowych. Warunkiem pozytywnego zaliczenia jest otrzymanie co najmniej 50% punktów możliwych do zdobycia. Zależność oceny od liczby punktów definiuje Regulamin Studiów. Dodatkowo zasady zaliczania przedmiotu i dokładne progi zaliczeniowe zostaną przekazane studentom na początku semestru z wykorzystaniem uczelnianych systemów elektronicznych oraz na pierwszych zajęciach (w każdej formie zajęć).

Treści programowe

W trakcie wykładów przedstawione zostaną zagadnienia związane planowaniem, przeprowadzaniem oraz analizą wyników testów penetracyjnych. Rozważane testy będą dotyczyć protokołów oraz urządzeń sieciowych. Z kolei w trakcie zajęć laboratoryjnych studenci będą sprawdzac w praktyce jak przeprowadzić proste tesy. Będą one realizowane w środowisku wirtualnym lub sieci rzeczywistej.

Tematyka zajęć

Wykłady:
1. Wprowadzenie do tematyki testów penetracyjnych
(podstawowe definicje, rodzaje testów penetracyjnych - białej-, czarnej- i szarej-skrzynki, techniki socjotechniczne, koszty i korzyści testu penetracyjnego, rekonesans pasywny, konieczność testów penetracyjnych, etapy testów penetracyjnych i wymagania klientów, zasady zachowania i ryzyka związane z testami penetracyjnymi, umowy prawne związane z testami penetracyjnymi).
2. Obowiązki licencjonowanego testera (LPT - Licensed Penetration Tester)
(obowiązki zawodowe LPT, normy prawne dla LPT, listy kontrolne zgodności niezbędne do przeprowadzenia testu penetracyjnego, zasady współpracy pomiędzy organizacją a testerami penetracyjnymi)
3. Planowanie i wykonywanie testów penetracyjnych, zewnętrzne i wewnętrzene testy penetracyjne
(faza planowania testów penetracyjnych, zespół testów penetracyjnych, lista kontrolna testów penetracyjnych, wymagania dotyczące testów penetracyjnych, rodzaje testów, mapy topologiczne sieci, fizyczna lokalizacja serwerów docelowych, różnorodność skanowań portów w sieci docelowej, rekord

DNS domeny, banery różnych serwerów, odpowiedzi ICMP, mapowanie sieci wewnętrznej, skanowanie portów poszczególnych maszyn, umieszczanie wirusów, trojanów i rootkitów na maszynie docelowej, MitM)
4. Zbieranie informacji i testy penetracyjne inżynierii społecznej
(kroki w procesie zbierania informacji, socjotechnika, zbieranie informacji o docelowej firmie, archiwalne strony)
5. Analiza podatności
(ocena podatności, klasyfikacja podatności, raport z oceny podatności, harmonogram oceny podatności)
6. Wyniki testów penetracyjnych oraz działania po testach
(elementy składowe raportu z testów penetracyjnych, jak dostarczyć raport klientowi, jak długo przechowywać informacje związane z testem penetracyjnym, rekomendacje zespołu testów penetracyjnych, plan działania na rzecz poprawy bezpieczeństwa, proces minimalizacji przypadków błędnych konfiguracji, wyciągnięte wnioski i najlepsze praktyki)
7. Zaawansowane exploity i narzędzia
Ćwiczenia laboratoryjne
1. Budowa śrdowiska testowego.
2. Narzędzia pentestera
3. Wykrywanie urządzeń w sieci oraz gromadzenie informacji
4. Testy penetracyjne w sieciach LAN (testy wewnętrzne)
- testy urządzeń sieciowych
-testy protokołów sieciowych
5. Narzędzia do automatycznego wykrywania podatności

Metody dydaktyczne

Wykład: prezentacja multimedialna uzupełniona przykładami i dodatkowymi objaśnieniami na tablicy. Wykłady prowadzone są zgodnie z zasadami wykładu tradycyjnego, w uzasadnionych przypadkach w formie wykładu konwersacyjnego.
Ćwiczenia laboratoryjne: prezentacja multimedialna, prezentacja ilustrowana przykładami podanymi na tablicy oraz wykonanie zadań podanych przez prowadzącego - ćwiczenia praktyczne.

Literatura

Podstawowa:
Matthew Hickey, Jennifer Arcuri, Warsztat hakera. Testy penetracyjne i inne techniki wykrywania podatności, Helion 2020
Gus Khawaja, Kali Linux i testy penetracyjne. Biblia, Helion 2022
Vijay Kumar Velu, Kali Linux i zaawansowane testy penetracyjne. Zostań ekspertem cyberbezpieczeństwa za pomocą Metasploit, Nmap, Wireshark i Burp Suite. Wydanie IV , Helion 2023
Uzupełniająca
serwisy poświęcone tematyce cyberbezpieczeństwa takie jak np. www.nist.gov

Uzupełniająca:
-

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	57	2,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	32	1,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	25	1,00