POLSKO-JAPOŃSKA AKADEMIA TECHNIK KOMPUTEROWYCH

SYLABUS PRZEDMIOTU

Nazwa przedmiotu:	**Testowanie bezpieczeństwa systemów IT**
Kod przedmiotu:	TBS
Kierunek / Profil:	Informatyka / praktyczny
Tryb studiów:	niestacjonarny
Rok / Semestr:	4 / 7
Charakter:	obowiązkowy
Odpowiedzialny:	mgr Adam Kassenberg
Wersja z dnia:	19.02.2026

1. Godziny zajęć i punkty ECTS

Wykłady	Ćwiczenia	Laboratori	Z prowa-dzącym	Praca własna	Łącznie	ECTS
30 h	—	30 h	60 h	65 h	125 h	**5**

2. Forma zajęć

Forma zajęć	Sposób zaliczenia
Laboratorium	Zaliczenie z oceną
Wykład	Egzamin

3. Cel dydaktyczny

Celem kursu jest nie tylko nauka teoretycznych podstaw zabezpieczania systemów IT, ale także zdobycie praktycznych umiejętności w identyfikacji i naprawie luk w zabezpieczeniach. Dzięki temu studenci będą lepiej przygotowani do zabezpieczania systemów informatycznych w rzeczywistych scenariuszach.

4. Treści programowe

1. 1. Wprowadzenie do testowania bezpieczeństwa
2. Cel i znaczenie testowania bezpieczeństwa.
3. 2. Metodologia testów penetracyjnych
4. Definicja testów penetracyjnych.
5. Różne podejścia i metodologie.
6. Etapy testów penetracyjnych: rozpoznanie, skanowanie, uzyskiwanie dostępu, utrzymanie dostępu, analiza i raportowanie.
7. Ćwiczenia praktyczne: Rozpoznanie i skanowanie w rzeczywistych scenariuszach.
8. 3. Metasploit
9. Wprowadzenie do narzędzia Metasploit.
10. Konfiguracja i podstawowe funkcje.
11. Przykłady wykorzystania Metasploit do testów penetracyjnych.
12. Ćwiczenia praktyczne: Wykorzystanie Metasploit do eksploatacji luk w zabezpieczeniach.
13. 4. Bezpieczeństwo aplikacji webowych
14. Najczęstsze zagrożenia i luki w zabezpieczeniach aplikacji webowych.
15. Przykłady ataków i ich skutki.
16. Techniki zabezpieczania aplikacji webowych.
17. Ćwiczenia praktyczne: Symulacja ataków na aplikacje webowe i implementacja zabezpieczeń.
18. 5. Kontrola dostępu do funkcji i danych
19. Definicja i znaczenie kontroli dostępu.
20. Najlepsze praktyki implementacji.
21. Przykłady problemów i ich rozwiązania.
22. Ćwiczenia praktyczne: Implementacja mechanizmów kontroli dostępu w aplikacjach.
23. 6. SQL Injection
24. Mechanizmy ataku SQL Injection.
25. Metody identyfikacji i zabezpieczania przed SQL Injection.
26. Przykłady ataków i ich skutki.
27. Ćwiczenia praktyczne: Wykrywanie i naprawa luk typu SQL Injection w aplikacjach.
28. 7. Cross Site Scripting (XSS)
29. Typy XSS: reflected, stored, DOM-based.
30. Techniki wykrywania i zabezpieczania przed XSS.
31. Przykłady ataków i ich skutki.
32. Ćwiczenia praktyczne: Symulacja ataków XSS i implementacja zabezpieczeń.
33. 8. Obsługa danych z niezaufanego źródła Znaczenie walidacji danych.
34. Techniki bezpiecznego przetwarzania danych.
35. Przykłady zagrożeń związanych z danymi niezaufanymi.
36. Ćwiczenia praktyczne: Implementacja walidacji danych w aplikacjach.
37. 9. Błędy konfiguracji Najczęstsze błędy konfiguracji systemów IT.

38. Metody identyfikacji i korekty.
39. Przykłady konsekwencji błędnej konfiguracji.
40. Ćwiczenia praktyczne: Audyt konfiguracji systemów i implementacja poprawnych ustawień.
41. 10. Testowanie typu Black Box
42. Definicja i cel testowania typu Black Box.
43. Techniki i narzędzia używane w testach Black Box.
44. Przykłady scenariuszy testowych.
45. Ćwiczenia praktyczne: Przeprowadzanie testów Black Box na rzeczywistych systemach.

5. Efekty kształcenia

Wiedza

- Student zna i rozumie metodologię i narzędzia używane do identyfikacji i eksploatacji luk w zabezpieczeniach (testy penetracyjne). Student rozumie działanie ataków SQL Injection oraz zna metody ich wykrywania i zapobiegania. Student zna i rozumie sposoby wykrywania i zabezpieczania przed atakami XSS.

Umiejętności

- Student potrafi korzystać z narzędzia Metasploit do testowania systemów. Student potrafi implementować i testować mechanizmy kontroli dostępu. Student potrafi przeprowadzić testy BlackBox na rzeczywistych systemach.

6. Kryteria oceny

- Studium przypadków
- Zadania problemowe
- Kryteria oceny
- Kolokwium pisemne.
- Skala ocen:
- Poniżej 50% - ndst
- Od 50% - dst
- Od 60% - dst+
- Od 70% - db
- Od 80% - db+
- Od 90% - bdb
- Skala ocen:
- Poniżej 50% - ndst
- Od 50% - dst
- Od 60% - dst+

- Od 70% - db
- Od 80% - db+
- Od 90% - bdb

7. Metody dydaktyczne

Wykład, laboratoria, praca własna studenta.

8. Literatura

Podstawowa:

- "Metasploit: The Penetration Tester's Guide, David Kennedy, Jim O'Gorman, Justin Brown i Peter Kim
- "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws", Dafydd Stuttard, Marcus Pinto
- "Hacking: The Art of Exploitation", Jon Erickson
- "Black Hat Python: Python Programming for Hackers and Pentesters", Justin Seitz

Uzupełniająca:

- "SQL Injection Attacks and Defense", Justin Clarke