# KARTA PRZEDMIOTU

## 1. Informacje ogólne

| | |
|---|---|
| **Nazwa przedmiotu i kod (wg planu studiów):** | Metodologie testów penetracyjnych: **D1_11** |
| **Nazwa przedmiotu (j. ang.):** | Penetration testing methodologies |
| **Kierunek studiów:** | Informatyka |
| **Specjalność/specjalizacja:** | Bezpieczeństwo systemów informatycznych |
| **Poziom kształcenia:** | studia I stopnia |
| **Profil kształcenia:** | praktyczny (P) |
| **Forma studiów:** | studia stacjonarne |
| **Obszar kształcenia:** | nauki techniczne |
| **Dziedzina:** | nauki techniczne |
| **Dyscyplina nauki:** | Informatyka |
| **Koordynator przedmiotu:** | mgr Radosław Gołąb |

## 2. Ogólna charakterystyka przedmiotu

| | |
|---|---|
| **Przynależność do modułu:** | kształcenie specjalnościowe |
| **Status przedmiotu:** | obowiązkowy |
| **Język wykładowy:** | Polski |
| **Rok studiów, semestr:** | III, 6 |
| **Forma i wymiar zajęć według planu studiów:** | stacjonarne - wykład 30 h, ćw. laboratoryjne 30 h |
| **Interesariusze i instytucje partnerskie (nieobowiązkowe)** | |
| **Wymagania wstępne / Przedmioty wprowadzające:** | Sieci komputerowe, Systemy operacyjne |

## 3. Bilans punktów ECTS

| | | stacjonarne |
|---|---|---|
| **Całkowita liczba punktów ECTS: (A + B)** | **4** | |
| **A. Liczba godzin wymagających bezpośredniego udziału nauczyciela z podziałem na typy zajęć oraz całkowita liczba punktów ECTS osiąganych na tych zajęciach:** | obecność na wykładach<br>obecność na ćwiczeniach laboratoryjnych<br>egzamin<br>udział w konsultacjach<br><br>**w sumie:**<br>ECTS | 30<br>30<br>2<br>5<br><br>67<br>2 |
| **B. Poszczególne typy zadań do samokształcenia studenta (niewymagających bezpośredniego udziału nauczyciela) wraz z planowaną średnią liczbą godzin na każde i sumaryczną liczbą ECTS:** | przygotowanie do ćwiczeń laboratoryjnych<br>wykonanie sprawozdań<br>przygotowanie do kolokwium<br>praca w sieci<br>przygotowanie do konsultacji<br>uzupełnienie/studiowanie notatek<br>studiowanie zalecanej literatury<br><br>**w sumie:**<br>ECTS | 10<br>20<br>10<br>5<br>5<br>5<br>5<br><br>60<br>2 |
| **C. Liczba godzin praktycznych / laboratoryjnych w ramach przedmiotu oraz związana z tym liczba punktów ECTS:** | udział w ćwiczeniach laboratoryjnych<br>praca praktyczna samodzielna<br><br>**w sumie:**<br>ECTS | 30<br>30<br><br>60<br>2 |

## 4. Opis przedmiotu

**Cel przedmiotu:**

Celem przedmiotu jest przedstawienie zagadnień związanych z planowaniem i przeprowadzaniem testów penetracyjnych systemów operacyjnych oraz sieci komputerowych.

**Metody dydaktyczne:** *wykład, praktyczne ćwiczenia laboratoryjne*

**Treści kształcenia**:

**Wykłady:**

1. Metody testowania zabezpieczeń systemów i sieci komputerowych.
2. Testy penetracyjne – metodologie przeprowadzania testów.
3. Symulacje włamań do systemów i sieci komputerowych.
4. Utwardzanie ochrony systemu operacyjnego, Application Armor.
5. Zarządzanie bezpieczeństwem, narzędzia analizy zabezpieczeń i monitoringu zabezpieczeń.
6. Sposoby analizy informacji zebranych w czasie testów penetracyjnych.
7. Przygotowanie raportów na podstawie informacji zebranych w czasie testów penetracyjnych.

**Ćwiczenia laboratoryjne:**

1. Rekonesans i skanowanie na przykładach systemów.
2. Ataki na hasła.
3. Wykorzystanie środowiska Metasploit.
4. Ataki na aplikacje WEB.

5. Kompleksowe testy penetracyjne oraz dokumentacja.

## 5. Efekty kształcenia i sposoby weryfikacji

| **Efekty kształcenia** | | |
|---|---|---|
| **Efekt przedmiotu** *(kod przedmiotu + kod efektu kształcenia)* | **Student, który zaliczył przedmiot (spełnił minimum wymagań)** | **Efekt kierunkowy** |
| | **Wiedza:** | |
| D1_11_W01 | 1. Ma wiedzę z zakresie podstaw przeprowadzania testów penetracyjnych. | K_W06 |
| D1_11_W02 | 2. Ma wiedzę na temat zagrożeń i sposobów zwiększania bezpieczeństwa w systemach i sieciach komputerowych. | K_W08 |
| D1_11_W03 | 3. Zna charakterystykę i podstawowe metodologie testów penetracyjnych. | K_W18 |
| | **Umiejętności** | |
| D1_11_U01 | 1. Student posiada umiejętności w zakresie planowania i przeprowadzania testów penetracyjnych. | K_U12 |
| D1_11_U02 | 2. Zna i umie zastosować główne metodologie testów penetracyjnych. | K_U15 |
| D1_11_U03 | 3. Potrafi zabezpieczyć system i sieć komputerową przed niepowołanym dostępem. | K_U16 |
| | **Kompetencje społeczne** | |
| D1_11_K01 | 1. Ma świadomość roli i znaczenia bezpieczeństwa przetwarzanych danych w przedsiębiorstwie, gospodarce i społeczeństwie. | K_K01 |
| D1_11_K02 | 2. Student rozumie potrzebę wykorzystania nabytej wiedzy na niezwykle szybko rozwijającym się rynku aplikacji. | K_K08 |

**Sposoby weryfikacji efektów kształcenia***:*
*(np. dyskusja, gra dydaktyczna, zadanie e-learningowe, ćwiczenie laboratoryjne, projekt indywidualny/ grupowy, zajęcia terenowe, referat studenta, praca pisemna, kolokwium, test zaliczeniowy**,** egzamin, opinia eksperta zewnętrznego, etc. Dodać do każdego wybranego sposobu symbol zakładanego efektu, jeśli jest ich więcej)*

| **Lp.** | **Efekt przedmiotu** | **Sposób weryfikacji** | **Ocena formująca** | **Ocena końcowa** |
|---|---|---|---|---|
| 1. | D1_11_W01<br>D1_11_W02<br>D1_11_W03<br>D1_11_U01<br>D1_11_U02<br>D1_11_U03 | egzamin | ocena z egzaminu - sprawdzian wiedzy i umiejętności | Ocena końcowa z egzaminu |
| 2. | D1_11_W01<br>D1_11_W02<br>D1_11_W03<br>D1_11_U01<br>D1_11_U02<br>D1_11_U03 | kolokwium zaliczeniowe | ocena z kolokwium - sprawdzian wiedzy i umiejętności | Ocena końcowa z laboratorium - średnia z ocen formujących |
| 3. | D1_11_U01<br>D1_11_U02<br>D1_11_U03<br>D1_11_K01 | ćwiczenia laboratoryjne | ocena sprawozdania z prac laboratoryjnych, ocena zaangażowania na zajęciach | |

| | | | | |
|---|---|---|---|---|
| | D1_11_K02 | | | |

**Kryteria oceny** (*oceny 3,0 powinny być równoważne z efektami kształcenia, choć mogą być bardziej szczegółowo opisane*)**:**

| **w zakresie wiedzy** | | **Efekt kształcenia** |
|---|---|---|
| Na ocenę 3,0 | Student uzyskał min. 50% wymaganej wiedzy w zakresie obowiązującego materiału. Student:<br>- Ma wiedzę z zakresie podstaw przeprowadzania testów penetracyjnych.<br>-Ma wiedzę na temat zagrożeń i sposobów zwiększania bezpieczeństwa w systemach i sieciach komputerowych.<br>- Zna charakterystykę i podstawowe metodologie testów penetracyjnych. | D1_11_W01<br>D1_11_W02<br>D1_11_W03 |
| Na ocenę 5,0 | Student zdobył powyżej 95% wymaganej wiedzy w zakresie obowiązującego materiału. Student:<br>- Ma wiedzę na temat cech protokołów sieciowych stanowiących podatności w systemach informatycznych.<br>- Ma wiedzę na temat konfiguracji systemów i urządzeń sieciowych zwiększających bezpieczeństwo.<br>- Potrafi dokonać wyboru odpowiedniej metodologii i uzasadnić ten wybór dla konkretnego systemu. | D1_11_W01<br>D1_11_W02<br>D1_11_W03 |
| **w zakresie umiejętności** | | **Efekt kształcenia** |
| Na ocenę 3,0 | Student uzyskał min. 50% wymaganych umiejętności w zakresie obowiązującego materiału. Student potrafi:<br>−Student posiada umiejętności w zakresie planowania i przeprowadzania testów penetracyjnych.<br>- Zna i umie zastosować główne metodologie testów penetracyjnych.<br>- Potrafi zabezpieczyć system i sieć komputerową przed niepowołanym dostępem. | D1_11_U01<br>D1_11_U02<br>D1_11_U03 |
| Na ocenę 5,0 | Student uzyskał min. 50% wymaganych umiejętności w zakresie obowiązującego materiału. Student potrafi:<br>- Student potrafi zaprojektować i zbudować sieć sensorową.<br>- Student potrafi samodzielnie wybrać metodologię i przeprowadzić testy penetracyjne.<br>- Umie wprowadzić zmiany zwiększające bezpieczeństwo systemu na podstawie analizy danych testów penetracyjnych. | D1_11_U01<br>D1_11_U02<br>D1_11_U03 |
| **w zakresie kompetencji społecznych** | | **Efekt kształcenia** |
| Na ocenę 3,0 | Student osiągną wymagane kompetencje społeczne na poziomie min. 50%. | D1_11_K01<br>D1_11_K02 |
| Na ocenę 5,0 | Student osiągną wymagane kompetencje społeczne na poziomie wyższym niż 90%. | D1_11_K01<br>D1_11_K02 |

**Student, który nie osiągnął zakładanych efektów kształcenia, nie zalicza przedmiotu.**

| **Kryteria oceny końcowej:** |
|---|

ocena z laboratorium:
ocena z kolokwium: 30 %
ocena ze sprawozdania: 50%
samodzielne wykonanie ćwiczeń laboratoryjnych: 15%
aktywność na zajęciach: 5%

ocena z egzaminu:
egzamin:100%

**Zalecana literatura** :

**Literatura podstawowa:**


1. Patrick Engebretson, Hacking i testy penetracyjne. Podstawy, Helion, Gliwice 2013
2. Muniz Joseph, Lakhani Aamir, Kali Linux Testy penetracyjne, Helion, Gliwice 2013
3. Adam Józefiok, Security CCNA 210-260. Zostań administratorem sieci komputerowych, Helion, Gliwice 2016
4. Thomas Wilhelm, Profesjonalne testy penetracyjne. Zbuduj własne środowisko do testów, Wydanie II, Helion, 2014


**Literatura uzupełniająca:**

Źródła internetowe: Serwisy internetowe poświęcone testom penetracyjnym

**Informacje dodatkowe:**

| **Dodatkowe obowiązki prowadzącego wraz z szacowaną całkowitą liczbą godzin:** |
|---|
| Konsultacje – 15 godzin |
| Poprawa prac projektowych – 10 godzin |
| Przygotowanie ćwiczeń laboratoryjnych - 5 godzin |
| W sumie: 30 godzin |