# Testy Penetracyjne

## Wprowadzenie

Arkadiusz Chrobot

Katedra Systemów Informatycznych

28 lutego 2024

# Plan

# Informacje kontaktowe

**Wykładowca:** dr inż. Arkadiusz Chrobot

**Numer pokoju:** 3.23, budynek D

**Termin konsultacji:**

**W tygodnie parzyste:** wtorek, 10:00 – 12:00

**W tygodnie nieparzyste:** środa, 14:00 – 16:00

**Numer telefonu:** 41 34-24-185

**Adres e-mail:** a.chrobot@tu.kielce.pl

**Strona WWW:** https://achilles.tu.kielce.pl/portal/Members/84df831b59534bdc88bef09b15e73c99

- Mike Chapple i David Seidl. *CompTIA© PenTest+ Study Guide*. New Jersey: SYBEX, 2022.
- David Kenedy i in. *Metasploit: Przewodnik po testach penetracyjnych*. Gliwice: Helion, 2013.
- Gus Khawaja. *Kali Linux i testy penetracyjne: Biblia*. Gliwice: Helion, 2022.
- Peter Kim. *Podręcznik pentestera: Bezpieczeństwo systemów informatycznych*. Gliwice: Helion, 2015.
- Gilberto Najera-Gutierrez i Juned Ahmed Ansari. *Kali Linux: Testy penetracyjne*. Wydanie trzecie. Gliwice: Helion, 2019.
- Michał Sajdak i in. *Bezpieczeństwo aplikacji webowych*. Kraków: Securitum, 2019.
- Michał Sajdak i in. *Wprowadzenie do bezpieczeństwa IT*. T. 1. Kraków: Securitum, 2023.

- *HackTheBox*. 2024. URL: https://www.hackthebox.com/.
- PCI DSS *Penetration Testing Guidance*. 2017. URL: https://listings.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf.
- *PortSwigger Web Security Academy*. 2024. URL: https://portswigger.net/web-security/all-labs.
- *Sekurak*. 2024. URL: https://sekurak.pl/.
- *The Penetration Testing Execution Standard*. 2014. URL: http://www.pentest-standard.org/index.php/Main_Page.

# Ostrzeżenia (prawne)

**Ostrzeżenie**

Testy penetracyjne (ang. *Penetration Tests*), w uproszczeniu, polegają na kontrolowanym atakowaniu systemu informatycznego. Wykonywanie ich bez zgody i wiedzy właściciela lub właścicieli takich systemów jest traktowane jako cyberprzestępczość i podlega określonym karom przewidzianych przez polskie prawo [9]. W zależności od konkretnego przypadku zastosowanie mają np. artykuły 267, 268, 268a, 269, 269a, 269b i 269c.

# Ostrzeżenia (prawne)

## Ochrona informacji i dostępu do systemów informatycznych

Art. **267** k.k.

§1. *Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.*

§2. *Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.*

§3. *Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.*

§4. *Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1–3 ujawnia innej osobie.*

§5. *Ściganie przestępstwa określonego w § 1–4 następuje na wniosek pokrzywdzonego.*

# Ostrzeżenia (prawne)

## Naruszenie integralności danych

Art. **268** k.k.

§1. *Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat* 2.

§2. *Jeśli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat* 3.

§3. *Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od* 3 *miesięcy do lat* 5.

§4. *Ściganie przestępstwa określonego w § 1–3 następuje na wniosek pokrzywdzonego.*

# Ostrzeżenia (prawne)

## Naruszenie integralności danych

Art. **268a** k.k.

§1. *Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat* 3.

§2. *Kto, dopuszczając się czynu określonego w § 1, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od* 3 *miesięcy do lat* 5.

§3. *Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.*

# Ostrzeżenia (prawne)

## Zakłócanie przetwarzania danych lub pracy systemu

Art. **269** k.k.

§1. *Kto niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności od* 6 *miesięcy do lat* 8.

§2. *Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając informatyczny nośnik danych lub niszcząc albo uszkadzając urządzenie służące do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych.*

# Ostrzeżenia (prawne)

## Zakłócanie przetwarzania danych lub pracy systemu

Art. **269a** k.k.

*Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie utrudnianie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od* 3 *miesięcy do lat* 5.

# Ostrzeżenia (prawne)

## Wytwarzanie, posiadanie, udostępnianie i sprzedaż narzędzi

Art. **269b** k.k.

§ 1. *Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełniania przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 1 lub 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające nieuprawniony dostęp do informacji przechowywanej w systemie informatycznym, systemie teleinformatycznym lub sieci teleinformatycznej, podlega karze pozbawienia wolności od* 3 *miesięcy do lat* 5.

§ 1a. *Nie popełnia przestępstwa określonego w § 1, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej przed popełnieniem przestępstwa wymienionego w tym przepisie albo opracowania metody takiego zabezpieczenia.*

§ 2. *W razie skazania za przestępstwo określone w § 1, sąd orzeka przepadek określonych w nim przedmiotów, a może orzec ich przepadek, jeśli nie stanowiły własności sprawcy.*

# Ostrzeżenia (prawne)

## Wyłączenia (np. *Lex Bug Bounty*)

Art. **269c** k.k.

*Nie podlega karze za przestępstwo określone w art. 267 § 2 lub art. 269a, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej albo opracowania metody takiego zabezpieczenia i niezwłocznie powiadomił dysponenta tego systemu lub sieci o ujawnionych zagrożeniach, a jego działanie nie narusza interesu publicznego lub prywatnego i nie wyrządziło szkody.*

# Ostrzeżenia (prawne)

## Podsumowanie

Przytoczone zapisy kodeksu karnego podlegają interpretacji zależnej od konkretnego przypadku, w którym mogą mieć zastosowanie także artykuły dotyczące czynu o znikomej szkodliwości społecznej (art. 1 § 2 k.k.), stronie podmiotowej (art. 8 i art. 9 § 1 k.k.), granicy wiekowej dla odpowiedzialności karnej (art. 10 § 1 k.k), formach stadialnych (art. 13 § 1 k.k) i zjawiskowych (art. 18 § 2 i § 3 k.k) oraz o wyłączeniu odpowiedzialności karnej (art. 26 k.k).
Osobną kwestią jest także jurysdykcja, która w przypadku cyberprzestępstw nie zawsze jest oczywista. Kraje inne niż Polska mają bardziej restrykcyjne prawo, które np. zabrania nawet posiadania oprogramowania, które może być użyte do popełnienie cyberprzestępstwa (np. *Computer Misuse Act* w Wielkiej Brytanii).

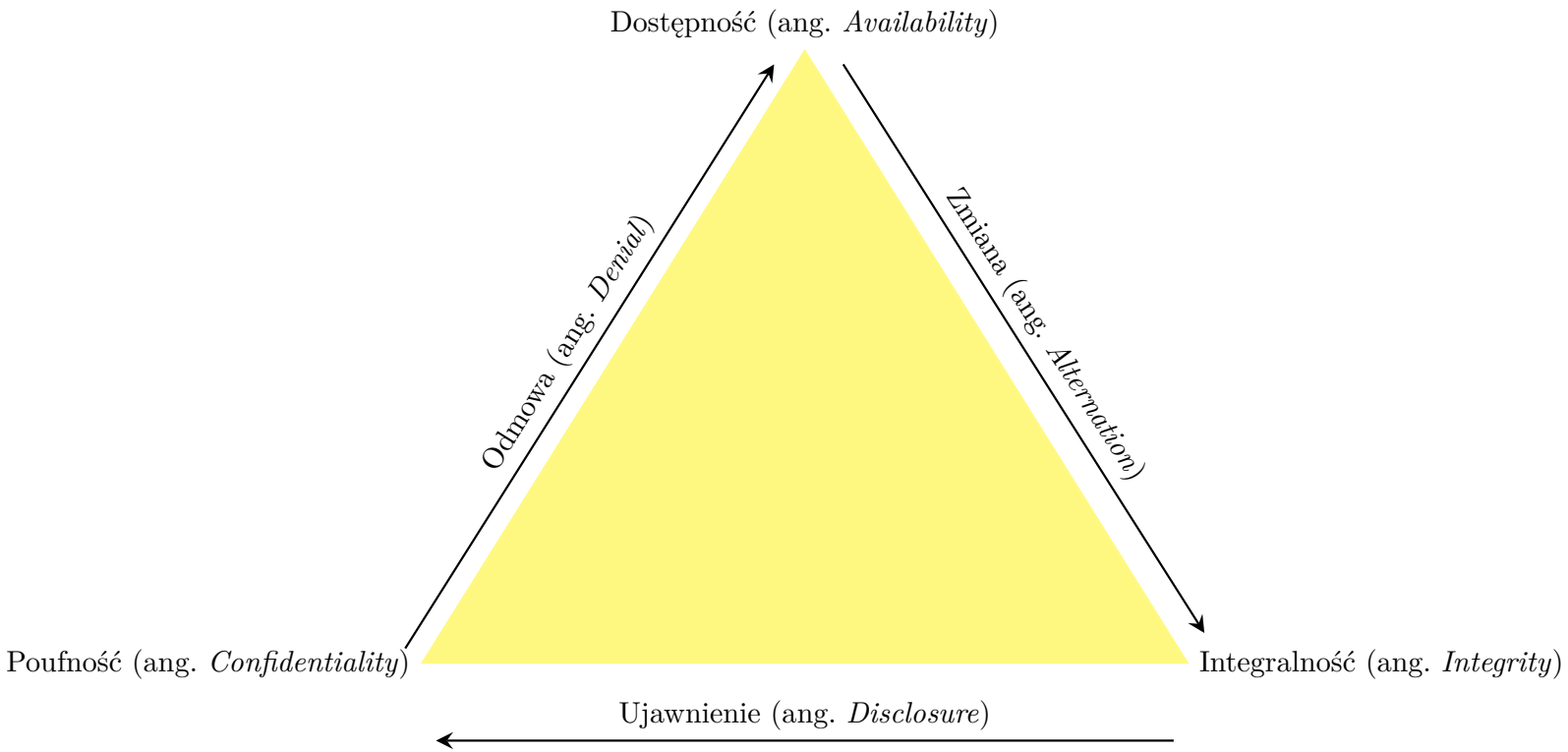
# Testy bezpieczeństwa

*Testy bezpieczeństwa* lub *testy zabezpieczeń* (ang. *security test*) są ogólnym pojęciem dotyczącym weryfikacji zastosowanych w systemach informatycznych mechanizmów, które mają zapobiegać naruszeniu poufności, integralności i dostępności aktywów. Ten termin obejmuje swoim znaczeniem wiele rodzajów testów, które można podzielić na dwie kategorie:

- defensywne testy bezpieczeństwa (ang. *defensive security tests*),
- ofensywne testy bezpieczeństwa (ang. *offensive security tests*).

Do tej drugiej kategorii zaliczane są *testy penetracyjne*, które również są pojęciem o bardzo pojemnym znaczeniu. Ogólnie, zmierzają one do podważenia spełniania przez system informatyczny wymienionych wcześniej wymagań bezpieczeństwa, poprzez wymuszenie *Ujawnienia* (ang. *Disclosure*) poufnych informacji, ich *Zmiany* (ang. *Alternation*) lub *Odmowy dostępu* (ang. *Denial*) do nich. Te cele testów penetracyjnych tworzą triadę DAD, która jest przeciwieństwem triady CIA (Rysunek 1).

# Testy bezpieczeństwa



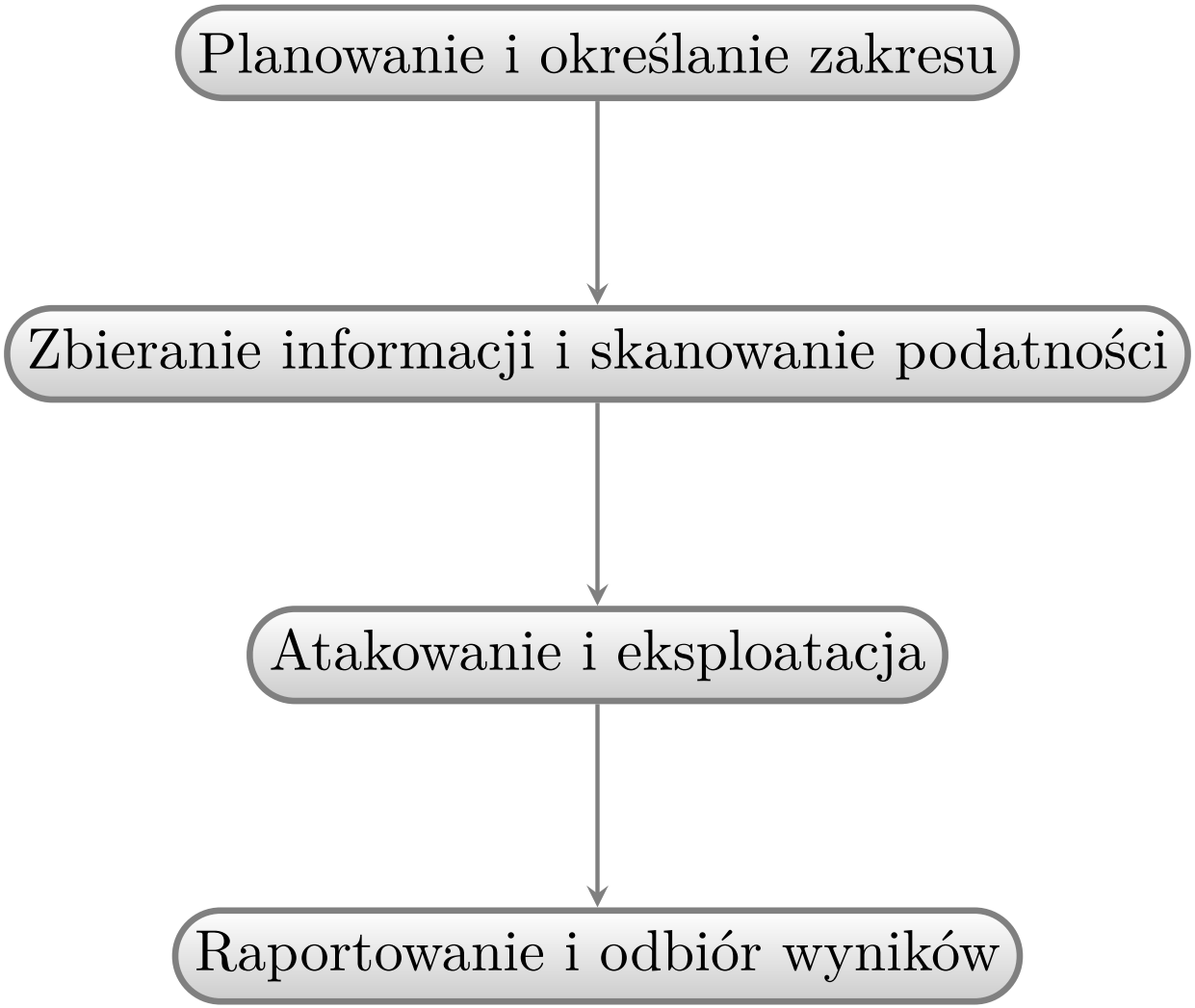

Rysunek: Triada DAD

# Testy penetracyjne

Głównym celem testów penetracyjnych jest ocena całościowego przygotowania systemów informatycznych i ich właścicieli na cyberatak. Pozwalają one sprawdzić, czy intruzi posiadający te same umiejętności i wiedzę jak testerzy, mogą uzyskać nawet częściowy dostęp do systemu. Jeżeli symulowany atak się powiedzie, to dokładana informacja o jego przebiegu może wskazać jakie środki zaradcze należy wprowadzić, aby przeciwdziałać rzeczywistej próbie przełamania zagrożeń. Ponadto, testy penetracyjne mogą wskazać podstawowe lub dodatkowe cele ataku potencjalnych intruzów.

Wysokopoziomowy przebieg prac w ramach testów penetracyjnych przedstawia Rysunek 2. Warto zwrócić uwagę, na pewną zbieżność tego schematu z *Łańcuchem ataku*, czyli modelem przebiegu włamania do systemu informatycznego, opracowanym przez firmę Lockheed Martin [1, 10]. W szczególności faza „Zbieranie informacji i skanowanie podatności" odpowiada etapowi „Rekonesans", a faza „Atakowanie i eksploatacja" etapom „Uzbrojenie" i „Działania dotyczące celów".

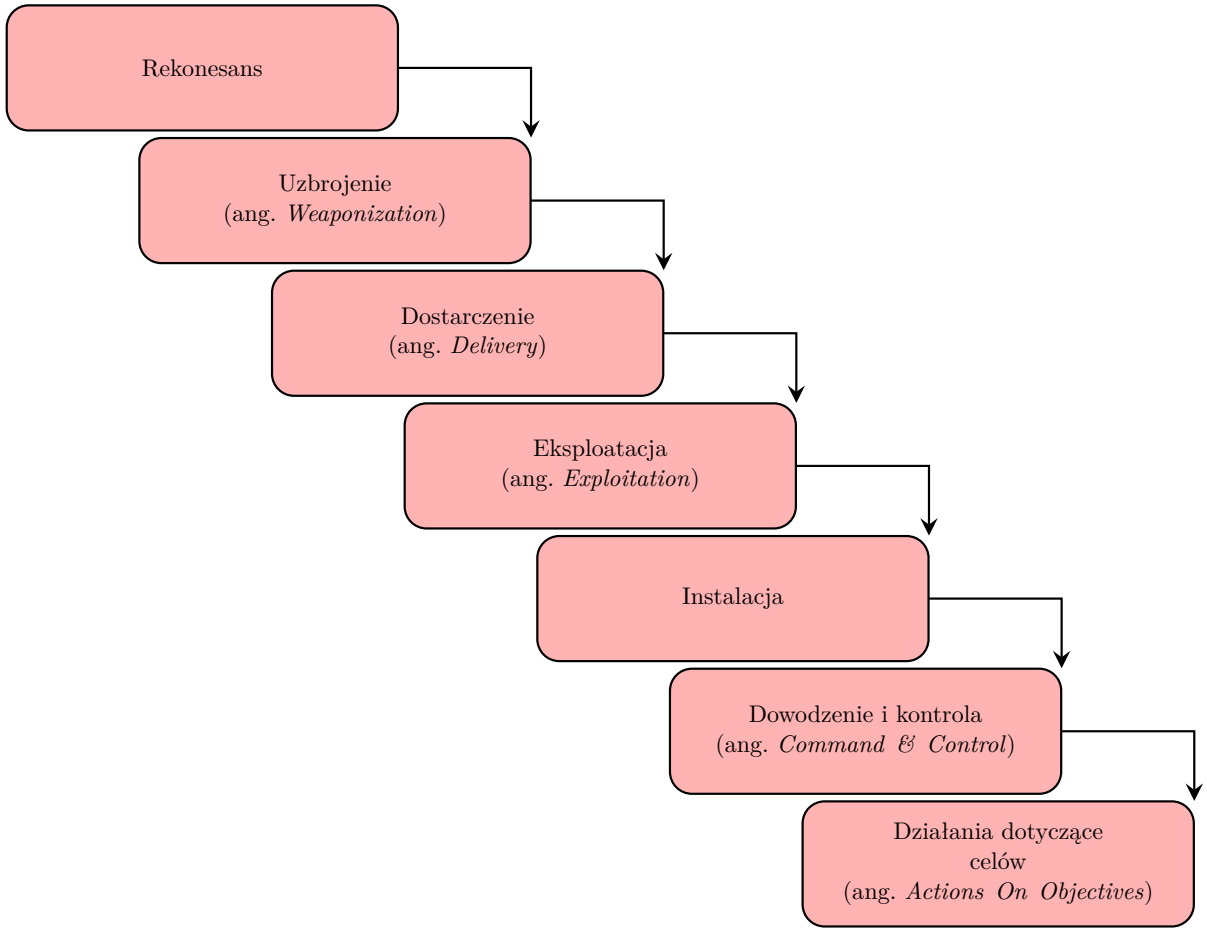
# Testy penetracyjne




Rysunek: Fazy testu penetracyjnego [1]

# Testy penetracyjne

## Łańcuch ataku (ang. *Cyber Kill Chain*)




Rysunek: Łańcuch ataku [1]

# Testy penetracyjne

## Podobne rodzaje testów

W cyberbezpieczeństwie stosowane są pokrewne do testów penetracyjnych działania:

**Skanowanie podatności** może występować jako samodzielna czynność, często zautomatyzowana.

**Audyt zgodności (ang. *Compliance-Based Assessment*)** weryfikacja zgodności zabezpieczeń z prawem i standardami.

**Celowa ocena (ang. *Objective-Based Assessment*)** weryfikacja zabezpieczenia konkretnego elementu systemu lub działania określonego mechanizmu zabezpieczającego.

**Kampania red-team (ang. *Read-Team Assesment*)** symulacja cyberataku, której celem jest ocena gotowości zespołów reagowania oraz ćwiczenie reakcji na incydenty.

**Threat Hunting (nie istnieje odpowiednia nazwa w języku polskim)** jest to aktywne szukanie dowodów na przełamanie zabezpieczeń systemu, przy założeniu, że ono nastąpiło, ale nie zostało jeszcze wykryte.

# Testy penetracyjne

## Klasyfikacja

Testy penetracyjne dzielą się na:

***Znanego środowiska*** nazywane również testami *Przezroczystej skrzynki* lub *Pełnej wiedzy*. Osoby przeprowadzające testy mają pełny dostęp do danych o weryfikowanym systemie, włącznie z informacjami uwierzytelniającymi.

***Nieznanego środowiska*** nazywane testami *Czarnej skrzynki* lub *Zerowej wiedzy*. Testerzy nie mają dostępu do żadnych informacji o weryfikowanym systemie. Muszą ją zdobyć samodzielnie, w początkowej fazie testów.

***Częściowej wiedzy*** nazywane także testami *Szarej skrzynki*. Osoby testujące mają dostęp tylko do części informacji o sprawdzanym systemie, np. zakres używanych adresów IP lub dane uwierzytelniające do konta z małym poziomem uprzywilejowania.

# Testy penetracyjne

## Zespoły

Wyróżnia się dwa typy zespołów, które mogą prowadzić testy bezpieczeństwa:

**Wewnętrzne** związane z podmiotem będącym właścicielem weryfikowanego systemu — mają dogłębną wiedzę, również dziedzinową na temat tego systemu, generują mniejsze koszty, ale mogą nie dostrzegać (lub *nie chcieć* zauważyć) pewnych zagrożeń.

**Zewnętrzne** spoza przedsiębiorstwa/organizacji, do której należy system — mogą dysponować większą wiedzą ekspercką i doświadczeniem z zakresu testów penetracyjnych oraz być bardziej obiektywni, jednak generują większe koszty.

Warto zauważyć pewne nieścisłości w terminologii. Pojęcie *zewnętrznego testu penetracyjnego* może oznaczać zarówno testy penetracyjne przeprowadzane z zewnątrz systemu przez dowolny rodzaj zespołu, jak i testy penetracyjne przeprowadzane przez zewnętrzny zespół. Podobny problem występuje w przypadku *wewnętrznych testów penetracyjnych*.

# Pytania

?

# Koniec

Dziękuję Państwu za uwagę!