

# BOT

Bezpieczeństwo oprogramowania i testy penetracyjne

## Wykład 1 - Wstęp

autor: dr inż. Mariusz Sepczuk

e-mail: [msepczuk@tele.pw.edu.pl](mailto:msepczuk@tele.pw.edu.pl)

# Plan wykładu

1. Cel przedmiotu
2. Plan gry
3. Cyberataki
4. Hacking i etyczny hacking
5. Testy penetracyjne
6. Prawo a hacking

# Cel przedmiotu

- Zapoznanie z podstawami przeprowadzania testów penetracyjnych
- Zapoznanie się z narzędziami używanymi do przeprowadzania testów penetracyjnych
- Zapoznanie się z problemami cyberbezpieczeństwa w systemach opartych o oprogramowanie
  - m.in. aplikacje WWW, aplikacje mobilne, cloud computing, sieciach WiFi
- Zapoznanie technikami zabezpieczenia się przed atakami wykorzystującymi oprogramowanie
- Zapoznanie się z podstawami wykorzystania użytkowników w cyberatakach (socjotechniki)

# Plan gry

## Wykład

- 15 wykładów wraz z kolokwium końcowym
- Wykłady odbywają się stacjonarnie w sali 118
- Do zdobycia 40 punktów za kolokwium

## Laboratorium

- 5 zajęć laboratoryjnych po 6 punktów = 30 punktów
- Laboratoria wykonywane są stacjonarnie

## Projekt

- Dwa rodzaje projektów: trzyosobowe i czteroosobowe
- Trzyosobowe: implementacja/konfiguracja wybranego zagadnienia związanego z bezpieczeństwem
- Czteroosobowe: cykl wytwórczy bezpiecznej aplikacji mobilnej
- Do zdobycia 30 punktów

# Harmonogram wykładu

| lp | Wykład  | Kiedy      | Kto |
|----|---|------------|-----|
| 1  | Wstęp   | 01.03.2022 | MS  |
| 2  | Rekonesans  | 08.03.2022 | MS  |
| 3  | Skanowanie  | 15.03.2022 | MS  |
| 4  | Wykorzystanie podatności                                  | 22.03.2022 | MS  |
| 5  | Ataki na uwierzytelnienie                                 | 29.03.2022 | MS  |
| 6  | Testy bezpieczeństwa sieci bezprzewodowych                | 05.04.2022 | MS  |
| 7  | Bezpieczeństwo aplikacji www                              | 12.04.2022 | MS  |
| 8  | Bezpieczeństwo infrastruktury w kontekście oprogramowania | 26.04.2002 | JB  |
| 9  | Bezpieczeństwo aplikacji mobilnych                        | 04.05.2022 | MS  |
| 10 | Utrzymanie dostępu i zacieranie śladów                    | 10.05.2022 | JB  |
| 11 | Testy e2e: od zamówienia do raportu                       | 17.05.2022 | MS  |
| 12 | Bezpieczeństwo wytwarzania oprogramowania                 | 24.05.2022 | JB  |
| 13 | Socjotechnika i ataki na użytkownika                      | 31.05.2022 | JB  |
| 14 | Inne obszary testów bezpieczeństwa                        | 07.06.2022 | MS  |
| 15 | Kolokwium końcowe   | 14.06.2022 | MS  |

MS: Mariusz Sepczuk

JB: Jędrzej Bieniasz

# Laboratorium

- W ramach laboratorium:
  - Zapoznasz się z narzędziami wykorzystywanymi w poszczególnych fazach testów penetracyjnych
  - Nauczysz się przeprowadzać poszczególne etapy testów penetracyjnych, aby finalnie móc przeprowadzić testy e2e
- Laboratorium oceniane będzie na podstawie sprawozdania stworzonego jako praca domowa (i ewentualnie krótkiego sprawdzianu wejściowego)
  - Laboratorium jest wykonywane w parach
  - Za laboratorium można uzyskać 6 punktów
    - Z każdego laboratorium należy uzyskać co najmniej 3 punkty
    - **-10% za każdy kolejny dzień spóźnienia w dostarczeniu sprawozdania**

# Laboratorium

| lp | Laboratorium   | kiedy                    | Kto   |
|----|--|--------------------------|-------|
| 1  | Skanowanie i przełamywanie zabezpieczeń                            | 25.03.2022               | MS/JB |
| 2  | Przepętnienie bufora   | 08.04.2022               | MS    |
| 3  | Ataki na aplikacje www   | 29.04.2022               | MS    |
| 4  | Kompleksowe testy bezpieczeństwa                                   | 20.05.2022               | MS    |
| 5  | Bezpieczeństwo wytwarzania aplikacji i wdrażania w infrastrukturze | 27.05 lub 3.06 lub 10.06 | JB    |

| 20.05.2022                  |     | MS  |    |    |    | Semestr 22L |          |    |                   |    |                 |                  |    |    |    | Następny semester |    |    |    |        |    |    |    |   |   |
|-----------------------------|-----|-----|----|----|----|-------------|----------|----|-------------------|----|-----------------|------------------|----|----|----|-------------------|----|----|----|--------|----|----|----|---|---|
| 27.05 lub 3.06<br>lub 10.06 |     | JB  |    |    |    |             | Kwiecień |    |                   |    | Maj             |                  |    |    |    | Czerwiec          |    |    |    | Lipiec |    |    |    |   |   |
| Poniedziałek                |     | 28  | 7  | 14 | 21 | 28          | 4        | 11 | 18                | 25 | 2               | 9                | 16 | 23 | 30 | 6                 | 13 | 20 | 27 | 4      | 11 | 18 | 25 | 1 |   |
| Wtorek                      |     | 1   | 8  | 15 | 22 | 29          | 5        | 12 | 19                | 26 | 3               | 10               | 17 | 24 | 31 | 7                 | 14 | 21 | 28 | 5      | 12 | 19 | 26 | 2 |   |
| Środa                       | 23  | 2   | 9  | 16 | 23 | 30          | 6        | 13 | 20 <sup>Pon</sup> | 27 | 4 <sup>Wt</sup> | 11               | 18 | 25 | 1  | 8                 | 15 | 22 | 29 | 6      | 13 | 20 | 27 | 3 | 1 |
| Czwartek                    | 24  | 3   | 10 | 17 | 24 | 31          | 7        | 14 | 21                | 28 | 5               | 12 <sup>Pi</sup> | 19 | 26 | 2  | 9                 | 16 | 23 | 30 | 7      | 14 | 21 | 28 | 4 | 1 |
| Piątek                      | 25  | 4   | 11 | 18 | L1 | 1           | L2       | 15 | 22                | L3 | 6               | 13               | L4 | 27 | 3  | 10                | 17 | 24 | 1  | 8      | 15 | 22 | 29 | 5 | 1 |
| Sobota                      | 26  | 5   | 12 | 19 | 26 | 2           | 9        | 16 | 23                | 30 | 7               | 14               | 21 | 28 | 4  | 11                | 18 | 25 | 2  | 9      | 16 | 23 | 30 | 6 | 1 |
| Niedziela                   | 27  | 6   | 13 | 20 | 27 | 3           | 10       | 17 | 24                | 1  | 8               | 15               | 22 | 29 | 5  | 12                | 19 | 26 | 3  | 10     | 17 | 24 | 31 | 7 | 1 |
|                             | N/P | N/P | N  | P  | N  | P           | N        | P  | N/P               | N  | P               | N                | P  | N  | P  | N                 | P  |    |    |        |    |    |    |   |   |

# Projekty realizowane w zespołach trzyosobowych

- Każdy zespół wybiera zagadnienie w ramach którego przeprowadzi analizę teoretyczną i wykona zadanie praktyczne: implementację lub konfigurację
- Etapy projektów:
  - Etap 0: stworzenie zespołów i wybór tematów => do 05.03.2022 23:59:59
  - Etap 1: analiza teoretyczna zagadnienia => do 03.04.2022 23:59:59
  - Etap 2: implementacja lub konfiguracja zagadnienia => do 29.05.2022 23:59:59
  - Etap 3: prezentacja projektów => 3.06.2022 lub 10.06.2022
- Ocenianie projektów:
  - Etap 1 – maks. 5 punktów za dokumentację tego co będzie do zrobienia
  - Etap 2 – maks. 20 punktów za dokumentację tego co zostało zrealizowane
  - Etap 3 – maks. 5 punktów za prezentację realizacji tematu
  - **Z każdego etapu należy uzyskać co najmniej połowę punktów**
  - **-10% punktów z danego etapu za każdy kolejny dzień spóźnienia**



# Projekty realizowane w zespołach czteroosobowych

- Każda grupa programuje aplikacje mobilną w architekturze klient-serwer
  - Jeden podgrupa (2 osoby programują), dwie przeprowadzają testy bezpieczeństwa aplikacji
  - Maksymalnie 4 tematy projektów (16 osób)
- Etapy projektów:
  - Etap 0: stworzenie zespołów i wybór tematów => do 05.03.2022 23:59:59
  - Etap 1: analiza teoretyczna zagadnienia => do 19.03.2022 23:59:59 (obie podgrupy)
  - Etap 2: implementacja zagadnienia => do 23.04.2022 23:59:59 (podgrupa kodująca)
  - Etap 3: testy penetracyjne => do 12.05.2022 23:59:59 (podgrupa testująca)
  - Etap 4: poprawa błędów => do 28.05.2022 23:59:59 (podgrupa kodująca)
  - Etap 5: retesty aplikacji => do 11.06.2022 23:59:59 (podgrupa testująca)

# Projekty realizowane w zespołach czteroosobowych

- Ocenianie projektów:
  - Etap 1 – maks. 5 punktów za dokumentację tego co będzie do zrobienia
  - Etap 2 – maks. 20 punktów za dokumentację tego co zostało zrobione, aplikację mobilną oraz serwer
  - Etap 3 – maks. 20 punktów za raport z testów penetracyjnych aplikacji
  - Etap 4 – maks. 5 punktów za poprawę błędów wynikających z raportu z testów penetracyjnych
  - Etap 5 – maks. 5 punktów za raport z retestów aplikacji
  - **Uwaga: Czas dowiezienia etapu jest niezwykle ważny !!!**
  - **Z każdego etapu należy uzyskać co najmniej połowę punktów**

# Projekty- pisanie dokumentacji

- Powinna być napisana językiem technicznym (bez sformułowań potocznych)
- Powinna odzwierciedlać sposób podejścia zespołu do problemu projektowego: analizę dostępnych możliwości rozwiązania problemu, uzasadnienie podejmowanych decyzji np. co do wyboru oprogramowania, bibliotek itp.
- Powinna zawierać m.in. takie elementy jak: szczegółową treść projektu, cele projektu, ogólne założenia projektu, opis architektury rozwiązania, opis sposobu działania (w przypadku aplikacji), opis najważniejszych funkcji/metod itp. wykonanej implementacji oraz bibliografię
  - Wikipedia nie jest dobrą pozycją bibliograficzną!
- Powinna zawierać referencje do pozycji literatury naukowej, standardów itp. (które zostaną umieszczone w bibliografii).
- Powinna "wyglądać" jak publikacja naukowo-techniczna pod względem estetycznym (formatowanie, justowanie, akapity itp. itd.)
  - Jest to „przetarcie” przed pisanem pracy dyplomowej

# Wybrane projekty trzyosobowe

1. Narzędzie do gromadzenia określonych danych (adresów email, telefonów, subdomen itp.) z wyszukiwarek
2. Testy bezpieczeństwa urządzeń typu router i switch
3. Wykorzystanie narzędzia scapy do przeprowadzania ataków
4. Narzędzie do analizy behawioralnej wykorzystujące monitoring Intencji Androida
5. Wtyczka do narzędzia BurpSuite wykrywająca wybrany atak
6. Testy bezpieczeństwa cloud computing
7. Testy bezpieczeństwa AD
8. Własny temat

# Projekty czteroosobowe

1. Aplikacja do zakupów internetowych
2. Aplikacja do zakupu biletu do kina
3. Aplikacja do wypożyczenia książek
4. Aplikacja do zamawiania jedzenia na wynos
5. Własny temat

# Warunki zaliczenia i ocenianie

- Aby zaliczyć przedmiot należy jednocześnie spełnić następujące wymagania:
  - Uzyskać co najmniej 15 punktów z laboratorium
  - Uzyskać co najmniej 15 punktów z projektu
  - Uzyskać co najmniej 21 punktów z kolokwium końcowego
  - Uzyskać co najmniej 51 punktów za cały przedmiot
- Skala ocen (standardowa):
  - (90;100] – 5
  - (80;90] – 4,5
  - (70;80] – 4
  - (60;70] – 3,5
  - [51;60] – 3
  - [0;50) – 2

# Konsultacje

- Prowadzący:
  - dr inż. Mariusz Sepczuk
    - Wykład, laboratorium, projekt
    - Konsultacje: wtorek godz. 17-18, pokój 475 (skrzydło ZCB)
      - Proszę o wcześniejszy kontakt przez MS Teams lub mail: [msepczuk@tele.pw.edu.pl](mailto:msepczuk@tele.pw.edu.pl)
  - mgr inż. Jędrzej Bieniasz
    - Wykład, laboratorium
    - Konsultacje: [J.Bieniasz@tele.pw.edu.pl](mailto:J.Bieniasz@tele.pw.edu.pl)
      - Preferowana forma online

# Co po BOTach ?

## Twój zakres obowiązków

- ✓ Wsparcie podczas wykonywania testów penetracyjnych aplikacji i przeglądu kodu
- ✓ Obsługa systemów do skanowania, testowania i zarządzania podatnościami w aplikacjach
- ✓ Udział w działaniach zespołu Bezpieczeństwa, zarządzaniu incydentami i podatnościami
- ✓ Proaktywny rozwój kompetencji, zdobywanie wiedzy w zakresie bezpieczeństwa aplikacji i metod przeprowadzania testów penetracyjnych

## Nasze wymagania

- ✓ Determinacja do pozyskiwania wiedzy z zakresu bezpieczeństwa aplikacji i metod przeprowadzania testów penetracyjnych
- ✓ Podstawowa znajomość metodyk tj. OWASP, OSSTMM
- ✓ Podstawowa znajomość przyczyn powstawania luk w aplikacjach webowych OWASP Top 10
- ✓ Podstawowa znajomość metod testowania aplikacji z wykorzystywaniem narzędzie tj. Burp OWASP ZAP
- ✓ Umiejętność dokumentowania i komunikowania wyników pracy
- ✓ Znajomość języka angielskiego co najmniej na poziomie B2
- ✓ Znajomość języka polskiego na poziomie C2

### Mile widziane

- ✓ Doświadczenie w pracy w obszarze testów penetracyjnych, CTF, bug bounty
- ✓ Umiejętność programowania w języku skryptowym (np. Python, bash)
- ✓ Znajomość mechanizmów działania protokołu HTTP



Przejdźmy do wykładu o testach  
penetracyjnych

# Internet jako integralna część biznesu i codziennego życia



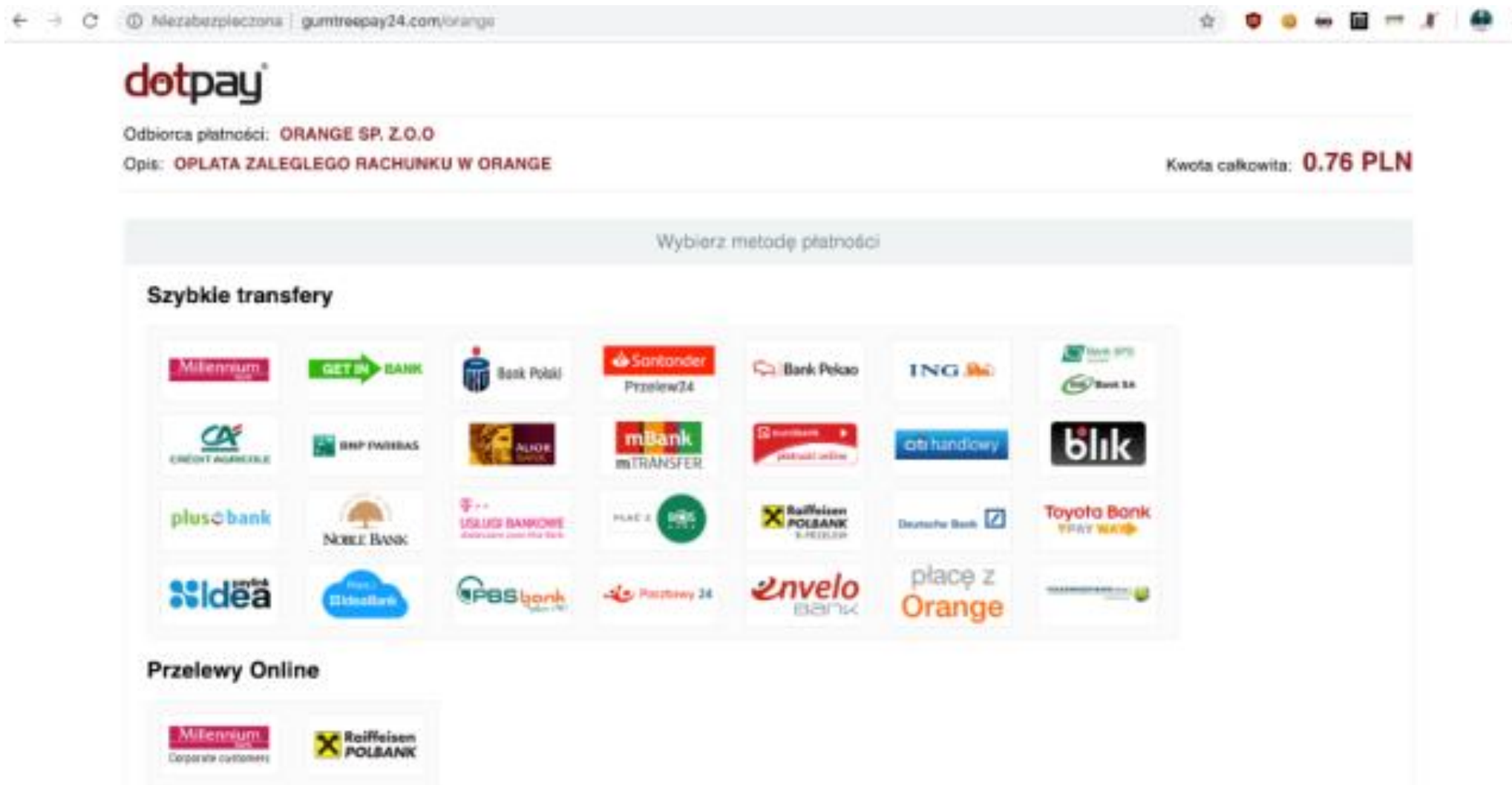
# Przykład 1: morele.net

- Wyciek danych osobowych
  - W tym loginów i haseł (md5crypt)
- Jak to wykorzystano
  - Przelewy pieniędzy z kont kupujących na morele.net
- UODO w związku z RODO nakłada karę w wysokości 2 830 410 PLN (660 tys. EUR)

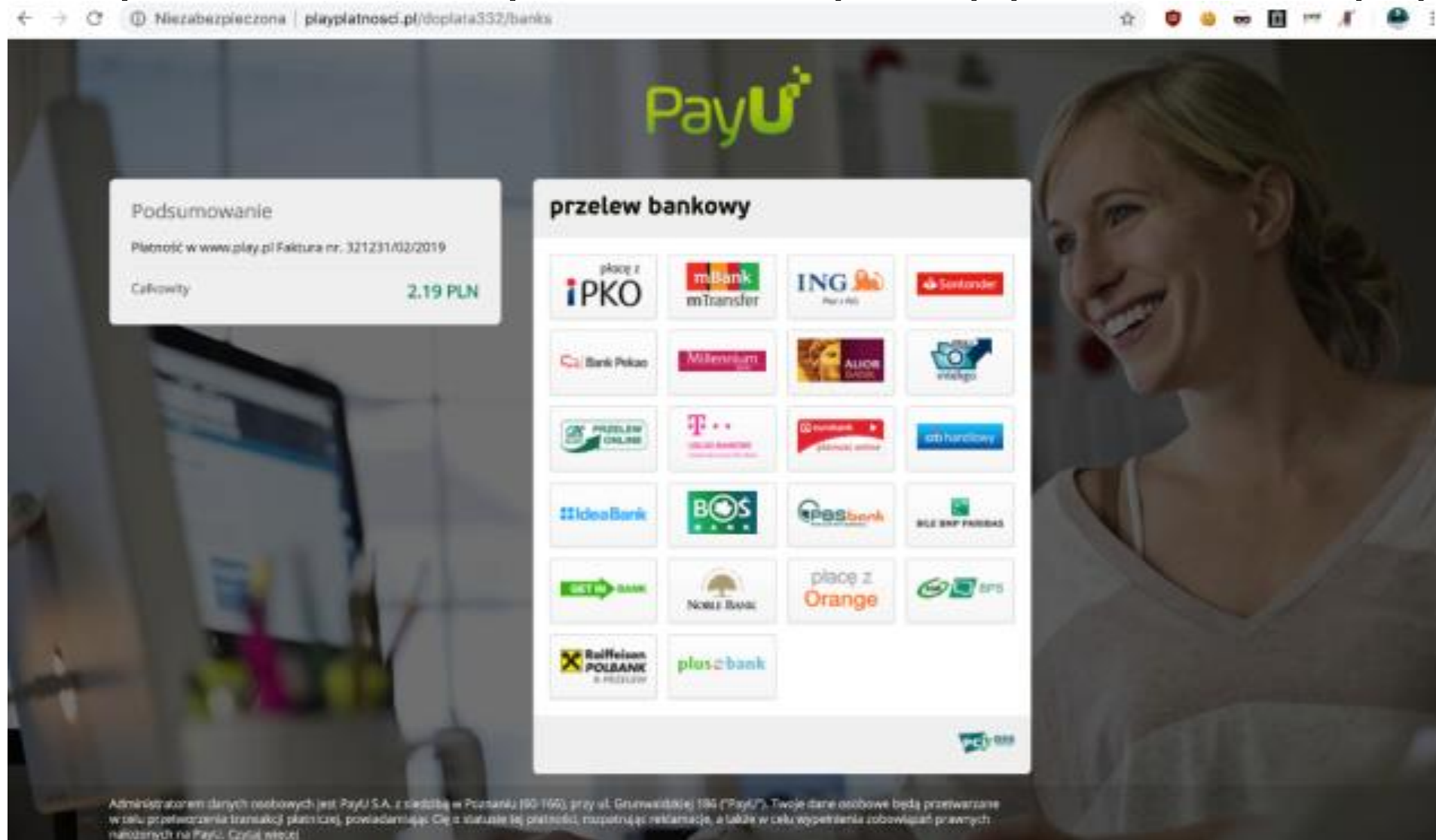


źródło: <https://niebezpiecznik.pl/>

# Przykład strony do fałszywej płatności (1/3)



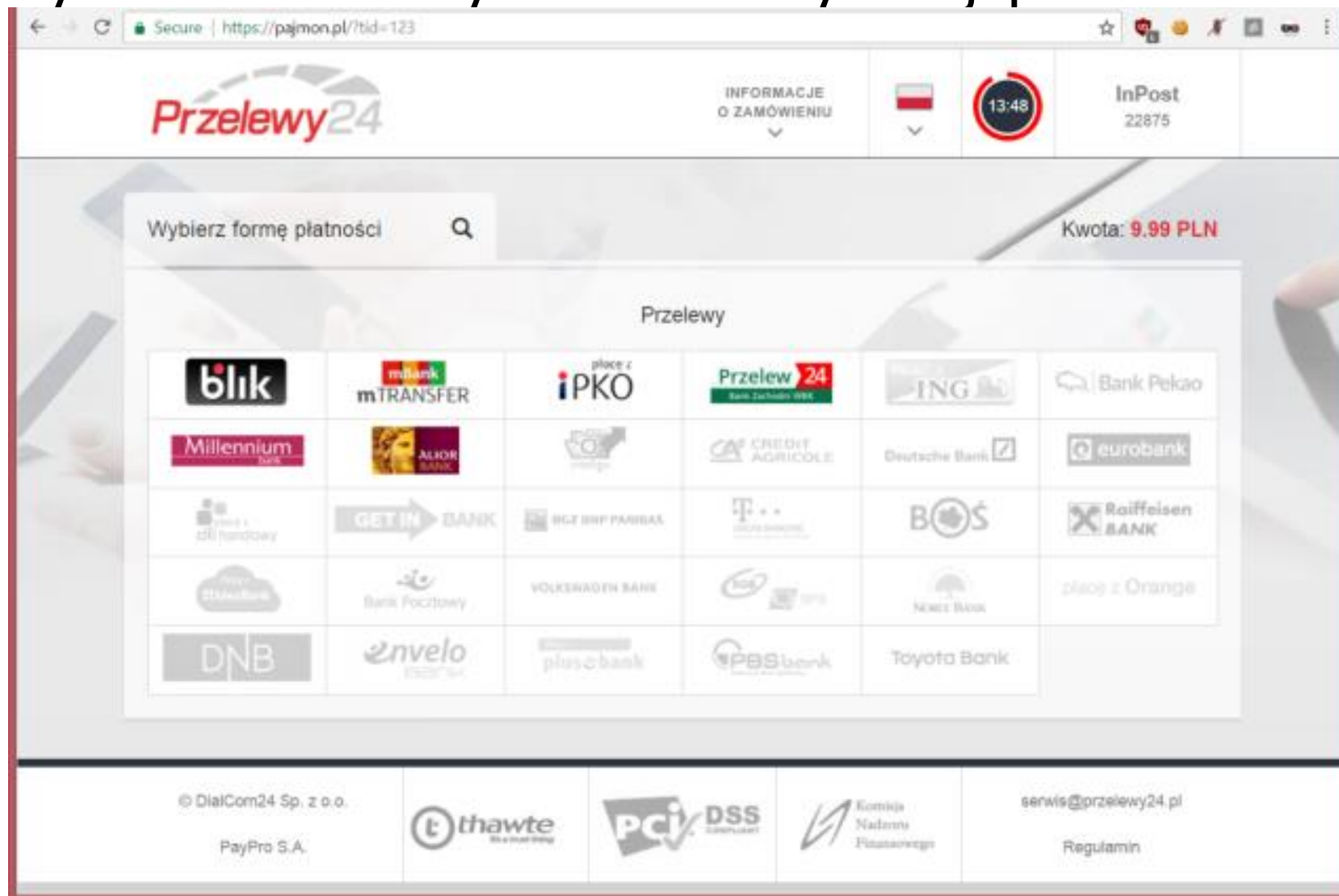
# Przykład strony do fałszywej płatności (2/3)



źródło: <https://www.mbank.pl>



# Przykład strony do fałszywej płatności (3/3)




## Przykład 2:

- Prawdopodobny wyciek danych osobowych
  - Imię i nazwisko, e-mail oraz adres zamieszkania
  - PESEL i numer dowodu
  - Historia 50 ostatnich transakcji
  - Informacje o lokatach i kredyty
  - Karty płatnicze (debetowe, kredytowe)
- Hacker w zamian za upublicznienie żąda od banku 200 000 PLN na dom dziecka
- Ostatecznie hacker zostaje złapany przez policję

# Przykład 3: **Linked**

- W 2012 roku na jednym z rosyjskich forów opublikowano 6,5 mln hashy haseł (SHA1)
- Po złamaniu 300k hashy dość często pojawiała się w nich fraza „linkedin”



**POLIMO**  
Joined: 31 Jul 2007  
Posts: 556  
Reputation: 395

Posted: Wed Jun 06, 2012 10:43 am Post subject:

Ok here my stuff !

**236 578** Cracked one ( propably more to come if i have time...)


cracked pass come from the start post, cause no left....

The join file is on pass format ( no hashe:pass cause i use JTR & on heavy file is taking to much time to past, so feel free to load my pass & past them)

Here the patern i find :

**linkedin  
link**

| 236578.txt   |             |
|--------------|-------------|
| Description: |             |
| Filename:    | 236578.txt  |
| Filesize:    | 2.24 MB     |
| Downloaded:  | 302 Time(s) |

 **Download**

[Back to top](#) [Profile](#) [PM](#)



## Przykład 4



Ryan Gallagher ✓  
@rj\_gallagher



Putin reportedly has a \$97 million luxury yacht called "Graceful". A group of Anonymous hackers on Saturday figured out a way to mess with maritime traffic data & made it look like the yacht had crashed into Ukraine's Snake Island, then changed its destination to "hell":

The screenshot displays the VesselFinder interface for a vessel identified as 'ANONYMOUS'. The vessel's status is 'Aground' as of February 26, 2022, at 01:09 UTC. It is located in Hamburg, Germany, with an ATD (Arrival Time Difference) of February 7, 06:26 UTC. The vessel's specifications include a speed of 0.0 kn, a course of 12.0°, and a draught of 3.8 m (max 3.8). The vessel's IMO number is 1011551, and its gross tonnage is 2685. The interface also shows a map of the Baltic Sea region with a red square highlighting the vessel's location near Snake Island. The vessel's navigation status is 'Drifting', and its position was received 11 minutes ago. The vessel's IMO/MMSI is 1011551 / 273294110, its callsign is FCKPTN, and its flag is Russia. The vessel's length and beam are 80 / 20 m.

| Navigation Status |                     |
|-------------------|---------------------|
| Position received | 11 mins ago         |
| IMO / MMSI        | 1011551 / 273294110 |
| Callsign          | FCKPTN              |
| Flag              | Russia              |
| Length / Beam     | 80 / 20 m           |

**Hamburg, Germany**  
ATD: Feb 7, 06:26 UTC

**MAP POSITION & WEATHER**

**ANONYMOUS**  
ETA: Apr 1, 14:00

| Speed: | Course: | Draught:        |
|--------|---------|-----------------|
| 0.0 kn | 12.0°   | 3.8 m (max 3.8) |

Status: **Aground**  
Last report: Feb 26, 2022 01:09 UTC

**Hamburg, Germany**  
ATD: Feb 7, 06:26 UTC

**PORT CALLS**

**WEATHER**

**VESSEL PARTICULARS**

| Gross Tonnage: | Built: | IMO number: |
|----------------|--------|-------------|
| 2685           | 2014   | 1011551     |

# Ważne pojęcia

**Podatność** (z ang. vulnerability) – słabość, która może zostać zaatakowana, skompromitowana i użyta jako punkt wejściowy np. do systemu

**Exploit** – naruszenie bezpieczeństwa systemu poprzez podatność (lukę)

**Ładunek** (z ang. payload) – część kodu exploita, która wykonuje zamierzoną złośliwą akcję np. przepełnienie bufora

**Atak „zero day”** – atak, który narusza bezpieczeństwo systemu, zanim deweloperzy nie stworzą i opublikują łatkę dla danej podatności

**Bot** – oprogramowanie, które może być kontrolowane zdalnie w celu wykonywania lub automatyzacji określonych zadań

**Zagrożenie** (z ang. Threat) – zdarzenie lub działanie, które może powodować naruszenie bezpieczeństwa, np. malware

# Triada CIA

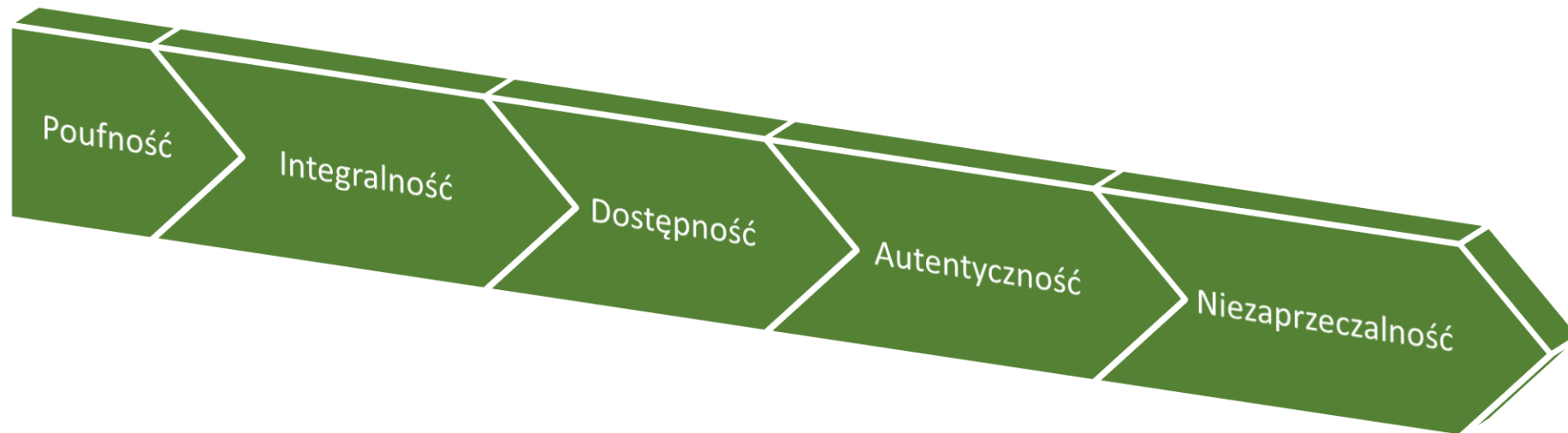
- Model triady CIA składa się z trzech elementów:
  - Integralność
  - Dostępność
  - Poufność



źródło: <https://medium.com/ediblesec/what-is-the-cia-triad-and-why-you-should-care-b7592cc2d89a>

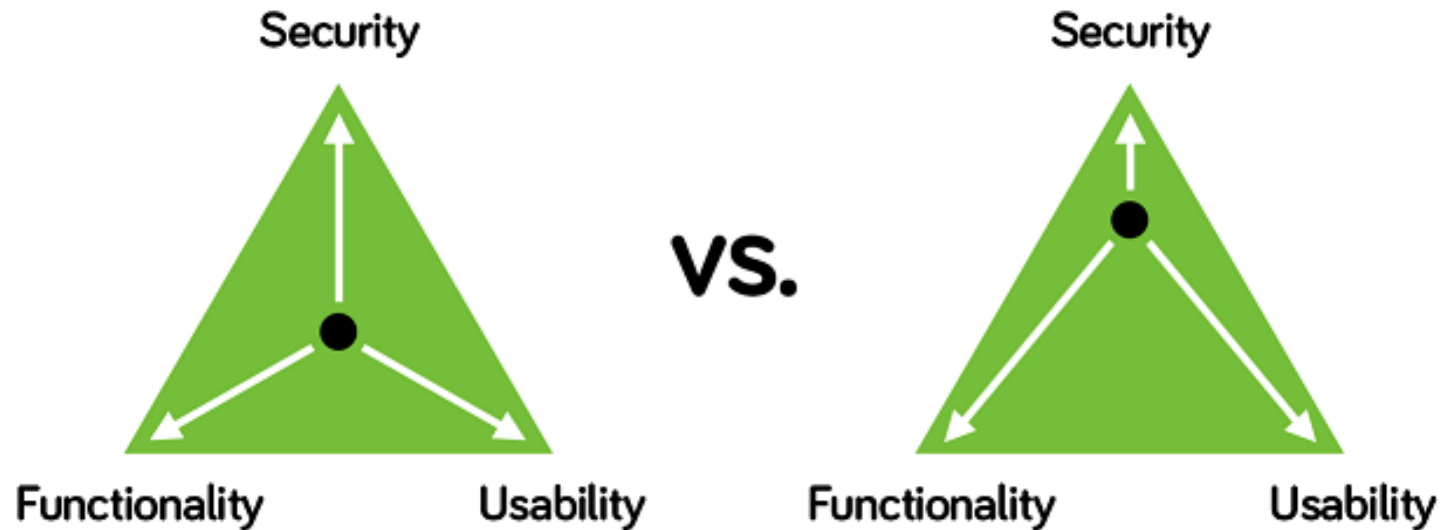
# Elementy bezpieczeństwa informacji

- Bezpieczeństwo informacji to stan ochrony informacji i infrastruktury, w którym prawdopodobieństwo kradzieży, manipulowania lub zakłócania usługi jest niskie lub dopuszczalne



# Security, Functionality & Usability Triangle

- Poziom bezpieczeństwa w dowolnym systemie może być zdefiniowany za pomocą wpływu trzech komponentów:



# Motywacja i cele ataków na dane

**Atak** = motywacja (cel) + metoda + podatność

- Motywacja wywodzi się z założenia, że system docelowy przechowuje lub przetwarza coś wartościowego, co prowadzi do zagrożenia atakiem na system
- Atakujący próbują różnorodnych technik i narzędzi aby wykorzystać podatność w systemie, aby osiągnąć swój założony cel
- Motywacje stojące za atakami:
  - Zakłócenie ciągłości biznesowej
  - Kradzież danych
  - Manipulacja danymi
  - Tworzenie chaosu i strachu poprzez zakłócenia infrastruktury krytycznej
  - Propagowanie religijnych lub politycznych przekonań
  - Zemsta
  - Zniszczenie reputacji celu
  - Realizacja celów militarnych

# Wektory ataków na dane

## Zagrożenia w chmurze obliczeniowej

- Chmura obliczeniowa jest koncepcją dostarczania na żądanie zasobów IT, w których mogą być przechowywane dane organizacji i klientów
- Błąd w aplikacji klienta może pozwalać atakującemu na dostęp do danych innego klienta

## Ataki APT (Advanced Persistent Threat)

- APT to atak, który skupia się na kradzieży cennych danych z hosta ofiary bez jej/jego świadomości
- Cechy: długotrwały, celowany, złożony, trudne do wykrycia

## Wirusy i robaki

- Wirusy i robaki są najbardziej rozpowszechnionym zagrożeniem sieciowym, które potrafią zarazić sieć już w kilka sekund
- Robaki propagują się samoistnie, w odróżnieniu od wirusów (bazują na infekcji plików)

## Zagrożenia mobilne

- Celem atakujących są urządzenia przenośne ze względu na zwiększone ich zapotrzebowanie w biznesie i życiu codziennym oraz relatywnie mniejszą kontrolę bezpieczeństwa

## Botnet

- Botnet jest ogromną siecią skompromitowanych systemów używanych przez intruza do przeprowadzania różnych ataków sieciowych np. DDOS

## Atak wewnętrzny

- Jest to atak przeprowadzony z sieci korporacyjnej lub pojedynczego komputera przez osobę która ma autoryzowany dostęp do sieci.

# Kategorie ataków

## Zagrożenia sieciowe

- Pozyskiwanie informacji
- Podłuchiwanie (sniffing i eavesdropping)
- MITM i przejęcie sesji
- Zatrwanie ARP i DNS
- Ataki DOS
- Ataki z wykorzystaniem haseł
- Ataki ze skompromitowanymi kluczami
- Ataki na FW i IDS

## Zagrożenia związane z hostem

- Złośliwe oprogramowanie
- Pozyskiwanie informacji
- Ataki z wykorzystaniem haseł
- Ataki DOS
- Wykonanie kodu
- Nieautoryzowany dostęp
- Podnoszenie uprawnień
- Backdoor
- Ataki związane z bezpieczeństwem fizycznym

## Zagrożenia aplikacyjne

- Nieprawidłowa walidacja danych IN/OUT
- Ataki na uwierzytelnienie i autoryzację
- Błędna konfiguracja bezpieczeństwa
- Ujawnienie informacji
- BOF, SQLI
- Ataki kryptograficzne
- Nieprawidłowe zarządzania sesją



# Czym jest hacking?

- Pojęcie hacking odnosi się do wykorzystywania podatności systemów i kompromitacji zabezpieczeń w celu otrzymania nieautoryzowanego dostępu do zasobów
- Hacking dotyczy modyfikacji systemów lub cech aplikacji w celu osiągnięcia korzyści, a przy tym pomijając oryginalny zamysł twórcy
- Hacking może zostać użyty do kradzieży, podkradania i redystrybuowania własności intelektualnej, co prowadzi do strat biznesowych

# Kim jest hacker?

1

- Inteligentna indywidualność posiadająca umiejętności „komputerowe” z możliwością tworzenia i badania oprogramowania i hardware’u

2

- Dla niektórych hacking jest to hobby (na którym można legalnie zarobić) sprawdzające na ile komputerów i do ilu sieci można się włamać

3

- Intencje hackerów mogą być uwarunkowane zdobycie wiedzy jaki i poszukiwaniu okazji do robienia nielegalnych rzeczy

# Typy hackerów

## Black hat

- Indywidualiści z niezwykłymi umiejętnościami komputerowymi, uciekający się do złośliwych lub destrukcyjnych aktywności
- Inaczej cracker

## White hat

- Indywidualiści posiadający umiejętności hackera i używający ich w defensywnie
- Inaczej security analyst

## Grey hat

- Indywidualności którzy pracują po stronie defensywy i ofensywy w zależności od okoliczności

## Suicide hat

- Indywidualności których celem jest zdobycie infrastruktury krytycznej i jednocześnie nie boją się organów ścigania czy kary

## Script kiddies

- Niedoświadczeni hackerzy którzy kompromitują systemu poprzez uruchomienie skryptów, narzędzi oraz oprogramowania tworzonego przez prawdziwych hackerów

## Cyber terrorist

- Indywidualności motywowani przekonaniami politycznymi lub religijnymi w celu wzbudzenia strachu przez wyrządzenie szkody sieci komputerowej w dużej skali

## State sponsored hackers

- Indywidualności zatrudniani przez rządy w celu uzyskania ściśle tajnych danych lub niszczenia systemów lub danych innych rządów

## Hacktivist

- Indywidualności którzy promują program polityczny przez hackowanie, w szczególności przez modyfikowanie lub wyłączanie stron www

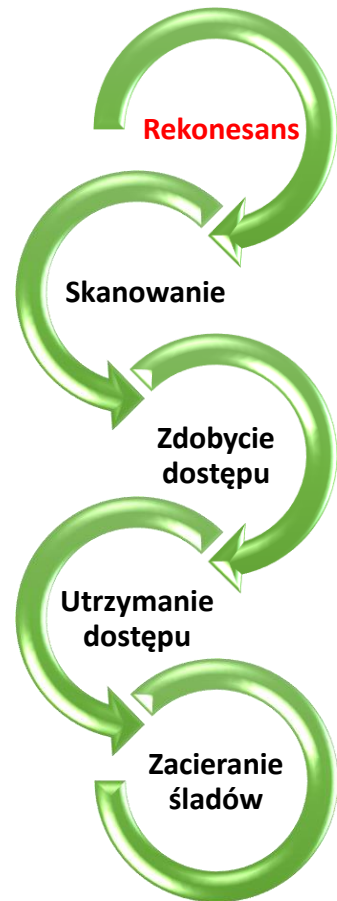
# Czym jest etyczny hacking?

- Etyczny hacking dotyczy się do wykorzystywania narzędzi, technik czy trików hackerskich do wykrywania podatności, aby zbadać bezpieczeństwo systemu
- Skupia się na symulacji technik używanych przez atakujących do weryfikacji istnienia podatności w systemie
- Etyczny hacker przeprowadza ocenę bezpieczeństwa organizacji za wyraźną zgodą odpowiednich jednostek organizacji

# Testy penetracyjne

- Testy penetracyjne to metoda oceny bezpieczeństwa systemu lub sieci poprzez symulację ataku na podstawie znalezionych podatności (tak jakby to zrobił hacker)
- Test penetracyjny nie tylko wskaże podatności danego zasobu, ale również udokumentuje w jaki sposób podatność można wykorzystać
- Rezultaty testów są dostarczane kompleksowo w postaci raportu, do zarządu i specjalistów techniczny

# Fazy testu penetracyjnego: rekonesans



- Rekonesans dotyczy fazy przygotowawczej, w której atakujący wyszukuje informacje o celu przed rozpoczęciem ataku
- Zakres rekonesansu może obejmować klientów danej organizacji, pracowników, procesy, sieć i systemy

## Rekonesans pasywny

- Pasywny rekonesans odnosi się do pozyskiwania informacji bez bezpośredniej interakcji z celem
- Np. przeszukiwanie Internetu czy prasy

## Rekonesans aktywny

- Aktywny rekonesans odnosi się do pozyskiwania informacji w bezpośredniej interakcji z celem
- Np. rozmowa telefoniczna z działem helpdesk lub z działem technicznym

# Fazy testu penetracyjnego: skanowanie



- Skanowanie dotyczy fazy przed atakiem, w której atakujący skanuje sieć w celu zdobycia specyficznych informacji na podstawie informacji z fazy rekonesansu
- Skanowanie może obejmować skanowanie portów, mapowanie sieci, narzędzia typu ping, skanowanie podatności
- Atakujący może wydobyć informację m.in. o aktywności hosta, portach, statusie portów, systemie operacyjnym hosta, szczegółach hosta do rozpoczęcia ataku

# Fazy testu penetracyjnego: zdobycie dostępu



- Zdobywanie dostępu dotyczy momentu kiedy atakujący uzyskuje dostęp do systemu operacyjnego lub aplikacji na komputerze lub w sieci
- Uzyskanie dostępu może się odbyć na poziomie systemu operacyjnego, sieciowym lub aplikacyjnym
- Atakujący może podwyższyć uprawnienia, aby jeszcze bardziej zwiększyć kontrolę nad systemem.
- Przykłady: łamanie haseł, BOF, DOS, SQL, przejęcie sesji, itp.

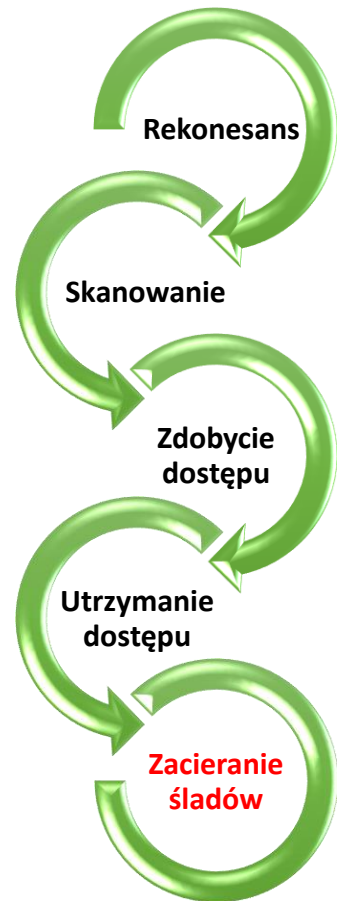


# Fazy testu penetracyjnego: utrzymanie dostępu



- Utrzymanie dostępu odnosi się do sytuacji kiedy atakujący chce zachować dostęp do przejętego systemu.
- W tym celu może wykorzystać np. backdoory, rootkity lub trojany.
- Atakujący mając dostęp do zaatakowanego systemu może dokonywać manipulacji danych, download'u i upload'u plików, a także zmian konfiguracyjnych.
- W konsekwencji może to prowadzić do dalszych ataków.

# Fazy testu penetracyjnego: zacieranie śladów



- Zacieranie śladów ma na celu ukrycie złośliwych działań atakującego.
- Intencje atakującego mogą dotyczyć: kontynuacji dostępu do zaatakowanego systemu, pozostaniu niezauważonym i niezłapanym, zniszczeniu dowodów na, które mogą wskazywać na atakującego, a w konsekwencji jego/jej oskarżenia
- Aby nie wzbudzać podejrzeń atakujący nadpisuje logi na poziomie serwera, systemu i aplikacji.

# Czy etyczny hacking jest potrzebny?

Aby pokonać atakującego musisz myśleć jako on !!!

- Dzięki etycznemu hackingowi:
  - Uniemożliwiasz hackerowi dostęp do danych organizacji
  - Poznajesz podatności systemu, dzięki czemu możesz określić jakie ryzyko ze sobą niosą i ewentualnie zmitygować je
  - Możesz przeanalizować siłę bezpieczeństwa organizacji wynikającą z polityk, ochrony infrastruktury sieciowej czy zachowań ludzkich

# Umiejętności etycznego hackera

## Techniczne umiejętności

- Ma szeroką wiedzę dotyczącą głównych systemów operacyjnych tj. Windows, Linux czy Unix
- Ma szeroką wiedzę sieciową dotyczącą koncepcji, technologii, oprogramowania i sprzętu
- Powinien być ekspertem komputerowych biegłym w dokumentacji technicznej
- Ma szeroką wiedzę dotyczącą zagadnień bezpieczeństwa i obszarów powiązanych
- Ma szeroką wiedzę techniczną do tego, aby przeprowadzić skomplikowany atak

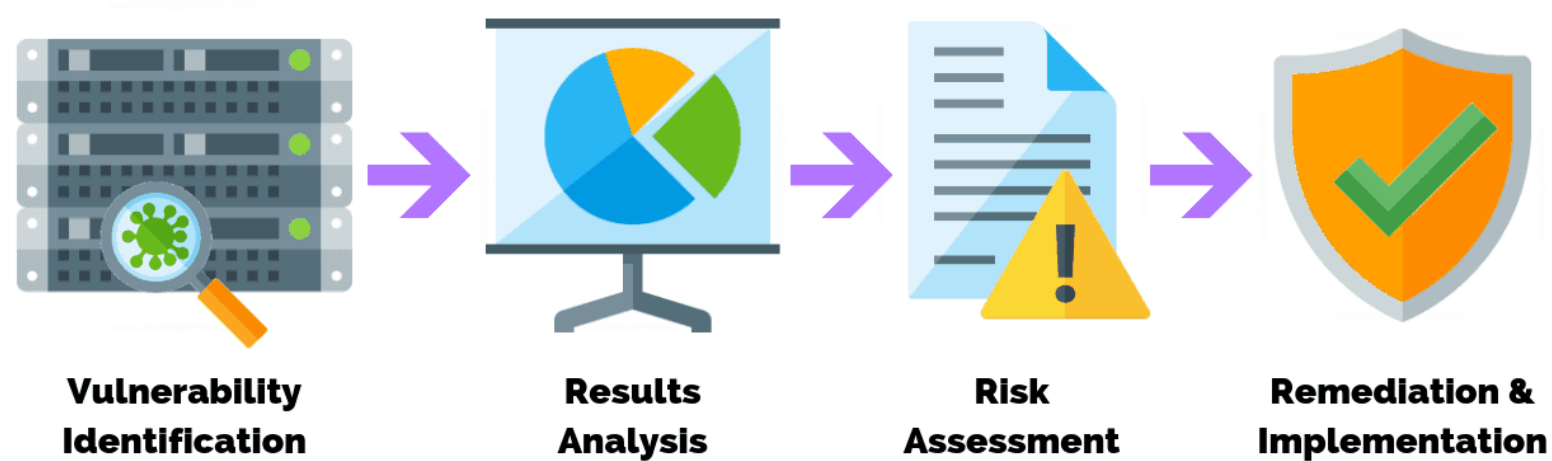
## Pozatechniczne umiejętności

- Zdolność szybkiego uczenia się i adaptowania się do nowych technologii
- Wysoko rozwinięty kodeks etyczny, umiejętności rozwiązywania problemów i komunikacji
- Zaangażowanie w politykę bezpieczeństwa organizacji
- Świadomość lokalnych praw i standardów

# Ocena podatności (Vulnerability Assessment)

- Ocena podatności jest badaniem zdolności systemu lub aplikacji, uwzględniając obecne procedury i kontrole bezpieczeństwa, do kompromitacji przy przeprowadzeniu ataku
- Rozpoznaje, mierzy i klasyfikuje podatności bezpieczeństwa w kategoriach systemu komputerowego, sieci i kanału komunikacyjnego
- Ocena podatności może być wykorzystana do:
  - Identyfikacji słabości, które mogą zostać wykorzystane
  - Przewidywania efektywności środków bezpieczeństwa stosowanych jako ochrona zasobów przed atakiem

# Proces oceny podatności



źródło: <https://purplesec.us/perform-successful-network-vulnerability-assessment/>

# Badania podatności (Vulnerability research)

- Proces odkrywania podatności i błędów, które dają możliwość ataku lub nadużycia systemu operacyjnego lub aplikacji
- Podatności są klasyfikowane na podstawie poziomów istotności (niska, średnia, wysoka) oraz zasięgu wykorzystania (lokalny, zdalny)
- Po co wiedza o podatnościach?
  - Pozyskiwanie informacji o trendach w bezpieczeństwie, zagrożeniach i atakach
  - Informowanie o podatnościach jeszcze przed wystąpieniem ataku
  - Wiedza jak podnieść się po ataku
  - Wiedza w jaki sposób uchronić się przed problemami bezpieczeństwa

# Audyt bezpieczeństwa vs ocena podatności vs testy penetracyjne

## Audyt bezpieczeństwa

- Audyt bezpieczeństwa sprawdza jedynie czy firma przestrzega procedur i polityki bezpieczeństwa

## Ocena podatności

- Ocena podatności skupia się na odkrywaniu w systemach informatycznych, ale nie pozwala zidentyfikować czy podatność można wykorzystać lub jaka skala nieprawidłowości pojawi się po wykorzystaniu podatności

## Testy penetracyjne

- Testy penetracyjne to metodyczne podejście do oceny bezpieczeństwa obejmujące audyt i ocenę podatności i pokazujące czy daną podatność można wykorzystać i w jaki sposób



# Blue teaming/Red teaming

## Blue teaming

- Podejście w którym grupa osób zajmująca się bezpieczeństwem przeprowadza analizy systemów w celu określenia odpowiednich i wydajnych kontroli bezpieczeństwa
- Blue team ma dostęp do wszystkich zasobów w organizacji
- Główna rola to detekcja i łagodzenie aktywności red team oraz przewidywanie w jaki sposób może wystąpić niespodziewany atak

## Red teaming

- Podejście w którym grupa etycznych hackerów przeprowadza testy penetracyjne systemów informatycznych z zerowym lub bardzo ograniczonym dostępem do zasobów organizacji
- Działania mogą się odbywać z ostrzeżeniem lub bez
- Proponuje się podejście wykrywania sieci, podatności i kontroli bezpieczeństwa z perspektywy dostępu atakującego do sieci, systemu czy informacji

# Typy testów penetracyjnych

## Czarna skrzynka (Black box)

Brak wcześniejszej  
wiedzy o testowanej  
infrastrukturze

Przykłady:

- Blind tests
- Double blind tests

## Biała skrzynka (White box)

Kompletna wiedza  
o testowanej  
infrastrukturze

## Szara skrzynka (Grey box)

Ograniczona wiedza  
o testowanej  
infrastrukturze

# Fazy testów penetracyjnych

## Faza przed atakiem

Planowanie i przygotowanie

Określenie metodyki

Zebranie informacji sieciowych

## Faza ataku

Przeprowadzenie ataki

Zdobycie celu

Podwyższenie uprawnień

Wykonanie, zagnieżdżenie, wycofanie

## Faza po ataku

Raportowanie

Czyszczenie

# Metodyki testów bezpieczeństwa

- Metodyki testów bezpieczeństwa lub testów penetracyjnych odnoszą się do metodycznego podejścia do wykrywania i weryfikacji podatności w mechanizmach bezpieczeństwa systemu informatycznego

|                                  |   |
|----------------------------------|---|
| OWASP                            | Open Web Application Security Project (OWASP) to niekomercyjny projekt bezpieczeństwa aplikacji, który pomaga organizacjom na zakupywanie, dewelopment i utrzymywanie narzędzi, aplikacji i wiedzy z zakresu bezpieczeństwa aplikacji www   |
| OSSTMM                           | Open Source Security Testing Methodology Manual (OSSTMM) to metodyka przeprowadzania wysokojakościowych testów bezpieczeństwa w obszarach: kontroli data control, fraud and social engineering, computer networks, wireless devices, mobile devices, phisical security, access control and various security processes |
| ISSAF                            | Information System Security Assessment Framework (ISSAF) to niekomercyjny projekt mający wspomóc specjalistów w przeprowadzeniu testów bezpieczeństwa. Misja ISSAF to: "research, develop, publish and promote a complete and practical generally accepted information systems security assesment framework "         |
| EP-Council<br>LPT<br>Methodology | Metodyka LPT jest ogonie zaakcentowanym framework'iem do przeprowadzania audytów bezpieczeństwa systemów informatycznych  |

# Prawo a hacking (1/3)

- „*Cracking* regulują dwa przepisy kodeksu karnego, dostarczając niezliczoną ilość problemów interpretacyjnych, których kilka postaram się zasygnalizować. Zgodnie z art. 267 § 1 kodeksu karnego przestępstwo popełnia **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**. Popełnienie przestępstwa *crackingu* zagrożone jest karą **grzywny, ograniczenia wolności albo pozbawienia wolności do lat 2.**”

# Prawo a hacking (2/3)

- „**Uzyskanie dostępu do informacji** będzie stanowić **przestępstwo jedynie w przypadku**, gdy będzie mieć charakter bezprawny, a więc gdy sprawca naruszy prawo innej osoby do dysponowania informacją i **uzyska do niej dostęp, nie będąc do tego uprawnionym**. Nie popełni przestępstwa osoba, która uzyska informacje wprowadzie dla niego nieprzeznaczone, jednak w sposób zgodny z prawem, np. policjant w przypadku prowadzenia podsłuchu zgodnie z obowiązującymi w tym zakresie przepisami, czy też pentester zaangażowany przez właściciela systemu.”

# Prawo a hacking (3/3)

- „Zgodnie z art. 267 § 2 kodeksu karnego tej samej karze podlega ten **kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego**. W tym przypadku już sam fakt uzyskania dostępu do systemu, bez konieczności przełamania lub ominięcia zabezpieczeń, stanowi przestępstwo, jeśli sprawca nie jest uprawniony, aby taki dostęp uzyskać. Jak należy rozumieć pojęcie systemu informatycznego? W prawie europejskim i międzynarodowym znajdziemy kilka krzyżujących się definicji. Również na gruncie prawa polskiego odmiennie definiuje się to pojęcie, czy to w ustawie o ochronie danych osobowych, czy też w ustawie o świadczeniu usług drogą elektroniczną.”

# Ważne na koniec!

Treści zawarte na tym przedmiocie służą jedynie do celów edukacyjnych i nie mają na celu skłanianie do przełamywania systemów lub zdobywania danych w nieautoryzowany sposób

Wiedzę zdobytą na tym przedmiocie wykorzystujesz na własną odpowiedzialność!!!



# BOT

Bezpieczeństwo oprogramowania i testy penetracyjne

## Wykład 1 - Wstęp

autor: dr inż. Mariusz Sepczuk

e-mail: [msepczuk@tele.pw.edu.pl](mailto:msepczuk@tele.pw.edu.pl)