

KRADZIEŻE, ATAKI I ŁAMANIE HASEŁ

JAKUB SIEŃSKI, KAROL WARDA, OLIWIA WITKOWSKA

DLACZEGO ŁAMANIE HASEŁ?

- Testowanie siły zabezpieczeń
- Audyty bezpieczeństwa
- Odzyskiwanie dostępu do zaszyfrowanych danych
- Edukacja w zakresie cyberbezpieczeństwa

RODZAJE ATAKÓW NA HASŁA



- Brute Force (siłowy)
- Słownikowy
- Hybrydowy
- Rainbow tables
- Ataki offline (na hashach)
- Ataki online (np. na serwery logowania)

JOHN THE RIPPER

- Jeden z najstarszych i najpopularniejszych programów do łamania haseł

Łamie hashe (MD5, SHA1, bcrypt itd.)

Wsparcie dla trybów słownikowych, brute-force i hybrydowych



HYDRA



Narzędzie do ataków online na protokoły logowania (SSH, FTP, HTTP, RDP itd.)

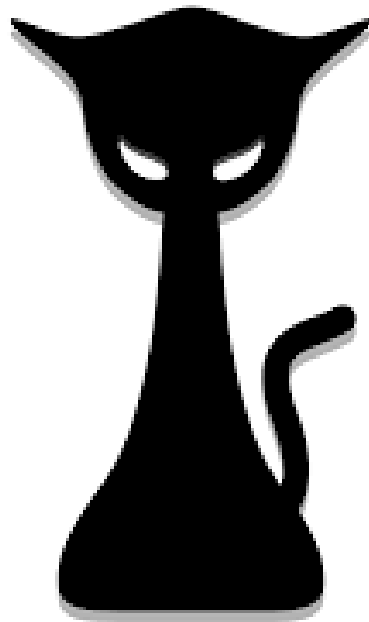
`hydra -l admin -P hasla.txt ftp://192.168.1.1`

```
(root@kali)~# hydra -l testuser -P /usr/share/wordlists/rockyou.txt -f localhost ssh
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-09-27 16:40:36
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://localhost:22/
[STATUS] 161.00 tries/min, 161 tries in 00:01h, 14344238 to do in 1484:55h, 16 active
[22][ssh] host: localhost login: testuser password: peanut
[STATUS] attack finished for localhost (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-09-27 16:41:37

(root@kali)~#
```

HASHCAT



Zaawansowane narzędzie do łamania haseł (offline)

Tryby:

- Brute-force
- Maski
- Reguły
- Słownikowy + reguły

HASH IDENTIFIER

Narzędzie do rozpoznawania typu hasha

Przydatne przy wstępie do łamania – wiedza, jaki algorytm zastosowano

[illegible]

SOCJOTECHNIKA - CO TO JEST?

Socjotechnika (social engineering) to technika manipulacji, która ma na celu skłonienie ofiary do ujawnienia poufnych informacji.

Ataki nie zawsze wymagają technologii - często wystarczy niewiedza lub zaufanie ofiary.

Najsłabszym ogniwem w systemie bezpieczeństwa zazwyczaj jest... człowiek.



SKĄD PRZESTĘPCY BIORĄ INFORMACJE?

- Media społecznościowe (Facebook, Instagram, TikTok, LinkedIn)
- Aplikacje randkowe (np. Tinder, Badoo)
- Fora internetowe, blogi, komentarze
- Publiczne rejestry i bazy danych
(np. LinkedIn → stanowisko pracy)

CELE ATAKU

- Odgadnięcie hasła (np. Imię dziecka + rok urodzenia)
- Przygotowanie phishingu dostosowanego do ofiary



PRZYKŁAD HASŁA OPARTEGO O DANE Z PROFILU



Ofiara: Zuzanna, rocznik 2005

Na profilu: pies o imieniu Luna, miasto Kraków

E-mail: zuzia2005@gmail.com

Potencjalne hasła:

Zuzia2005

Luna2005

Krakow05

LunaZuzia

Wszystkie to słabe hasła oparte o łatwo dostępne informacje. Można je zgadnąć lub wykorzystać w ataku słownikowym

GUESSING - JAK DZIAŁA?

Jest to atak polegający na próbie zgadywania haseł

Podstawą do zdobycia hasła ofiary mogą być np:

- Dane personalne - imiona, hobby, zawód, itp.
- "Podpowiedzi" - kartki na monitorze, pliki z hasłami
- Bazy danych - zbiór z różnych systemów, wycieki z internetu



GUESSING – JAK ZARADZIĆ

- Ustawiaj silne hasła niepowiązane ze sobą
- Nie zapisuj haseł do niezabezpieczonych plików (np. `.txt`)
 - Również w widocznych miejscach (np. Karteczka na monitorze)
- Jako admin: ustaw liczbę prób (ang. **Three strike method**)



PHISHING - JAK DZIAŁA?

Atak polega na wysłaniu fałszywego maila podszywającego się pod znaną instytucję.

Celem jest:

- wyłudzenie loginu i hasła,
- zmuszenie do kliknięcia złośliwego linku,
- przekonanie ofiary do instalacji malware.

Elementy typowego phishingu:

- Logo znanej firmy (np. banku)
- Pilna wiadomość („Twoje konto zostanie zablokowane!”)
- Link prowadzący na fałszywą stronę logowania



PRZYKŁAD PHISHINGU – FAŁSZYWA PROMOCJA ALLEGRO SMART

- Fałszywy nadawca: onlines@frankkoch.club – dziwna, niepowiązana domena.
- Zbyt dobra oferta: „Darmowe dostawy dla wszystkich” – atrakcyjna oferta mająca wywołać impulsowe kliknięcie.
- Pilny ton i odniesienie do sytuacji społecznej: W treści padają sformułowania typu „apel o pozostanie w domach” – to typowe wykorzystanie emocji i aktualnych wydarzeń do manipulacji.
- Podobieństwo graficzne do oryginalnego Allegro: Kolory, logo i format wiadomości są bardzo zbliżone do oryginału – to tzw. „brand impersonation”.
- Fałszywe linki: Przycisk AKTYWUJ zapewne prowadzi do podstawionej strony logowania, która może przechwytywać dane.



PHISHING - JAK ZARADZIĆ

- sprawdzaj czy twój system nie posiada niepożądanych aplikacji (wirusów)
- Bądź czujny na wyłudzenia
- Sprawdzaj domeny przed logowaniem



CRACKING - JAK DZIAŁA

Jest to atak polegający na dekrypcji, bądź odgadnięciu wykradzionych haseł

Metoda Brute-Force:

- Pozyskanie bazy haseł z systemu (zazwyczaj hasła są **hashowane**)
- Pobranie publicznej bazy haseł
- Krok po kroku: hashuj hasło z publicznej bazy, i porównuj do haseł z zahashowanej
- Jeśli są sobie równe - znalazłeś hasło!



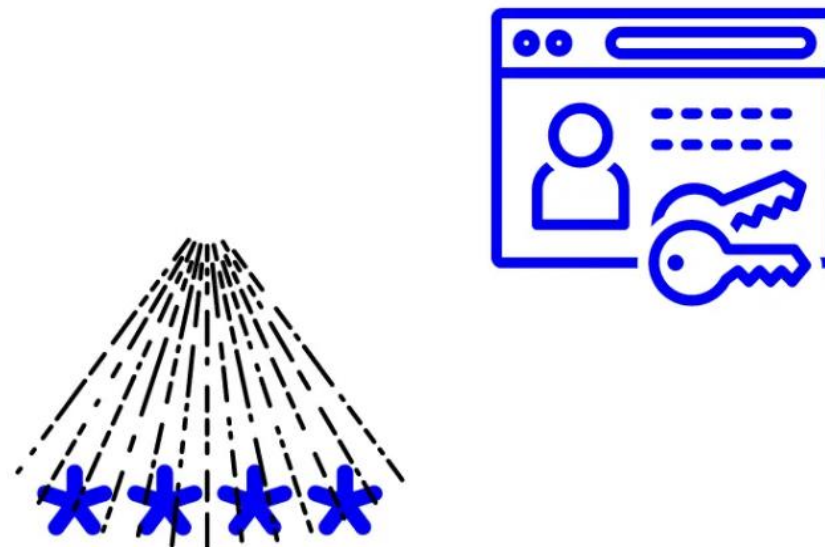
SPRAYING\STUFFING - JAK DZIAŁA?

Ataki polegające na próbach złamania haseł kont\systemów

Celem jest dostanie się do jak największej liczby kont wykorzystując ogólnie dostępne środki (np. Baza haseł, które wyciekły do sieci)

Krok po kroku:

- Zbierz publicznie dostępne hasła
- Sprawdź hasło raz na konto/system
- Powtarzaj dla każdego hasła, aż zadziała



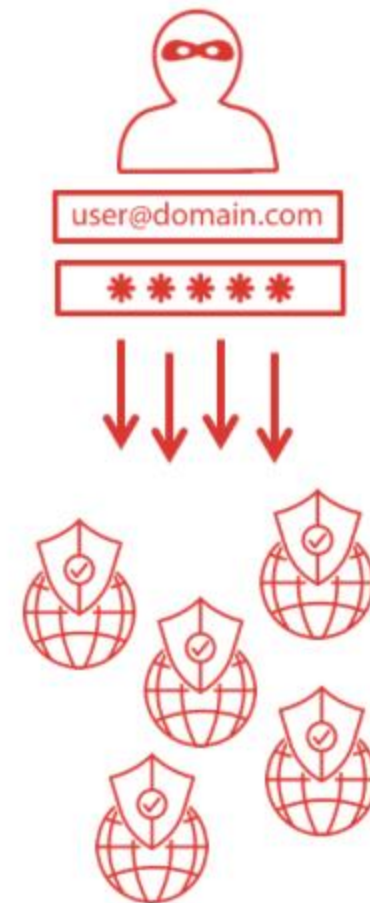
SPRAYING\STUFFING CD.

Metody te są uciążliwe, ponieważ ciężiej je wychwycić:

- Unikają metod zabezpieczeń przed włamaniami (**Three Strike Method**)
- Nie wychylają się poza normę - jedna próba na konto\system i przechodzą dalej

Jak zaradzić przed takimi atakami?

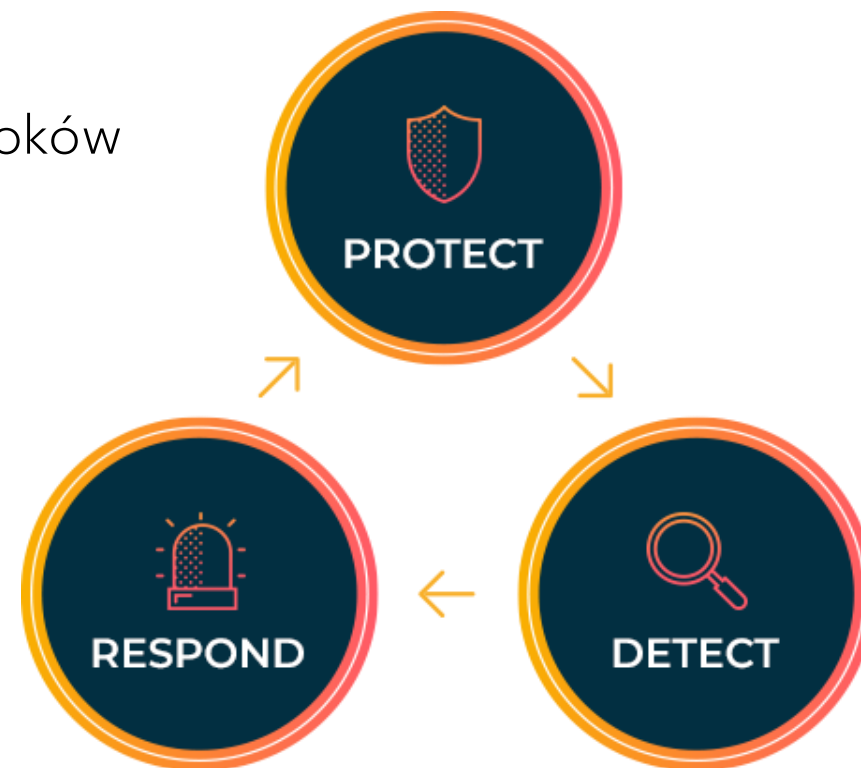
- Nie używać słabych haseł
- Unikać powtarzania tych samych haseł na różnych kontach



CYBERBEZPIECZEŃSTWO W 3 KROKACH:

W cyberbezpieczeństwie stosowana jest metoda 3 kroków by zaradzić włamaniom:

- Protect
- Detect
- Response



CYBERBEZPIECZEŃSTWO - PROTECT

Czyli wszystko związane z zabezpieczeniem haseł:

- Testuj siłę haseł oraz ich bezpieczeństwo (czy są w publicznych bazach)
- Używaj 1 hasła na 1 konto

Używaj dodatkowych zabezpieczeń (2FA):

- Sms
- Email
- Authentication app



CYBERBEZPIECZEŃSTWO-DETECT

Czyli sposoby na odnajdywanie prób włamań

- Multiple fails by time:
 - Dużo logowań w małym czasie = zły aktor, próba sprayingu
- Multiple fails by accounts
 - Podobnie tylko jest to próba stuffingu



CYBERBEZPIECZEŃSTWO- RESPONSE

Czyli jak odpowiedzieć na ataki

- Blokuj podejrzane adresy IP
- Zablokuj skompromitowane konto na czas rozpatrzenia
- Wymuś zmianę hasła na skompromitowanym koncie



CO TO JEST KRYPTOGRAFIA?

Kryptografia to nauka o zabezpieczaniu informacji. Pomaga chronić nasze dane, tak by nie dostały się w niepowołane ręce.

Umożliwia:

- 🔒 ukrycie treści (szyfrowanie)
- ✅ potwierdzenie tożsamości (autoryzacja)
- 📄 zabezpieczenie przed zmianą danych (integralność)



5 FILARÓW BEZPIECZEŃSTWA DANYCH

🧱 **Poufność** – tylko upoważnione osoby mogą zobaczyć dane

🌀 **Integralność** – dane nie zostały zmienione przez nikogo

🕒 **Dostępność** – dane są dostępne, gdy są potrzebne

✅ **Autentyczność** – wiadomo, kto wysłał lub zalogował się

✍️ **Niezaprzeczalność** – nikt nie może zaprzeczyć, że coś zrobił






JAK CHRONIMY DANE?

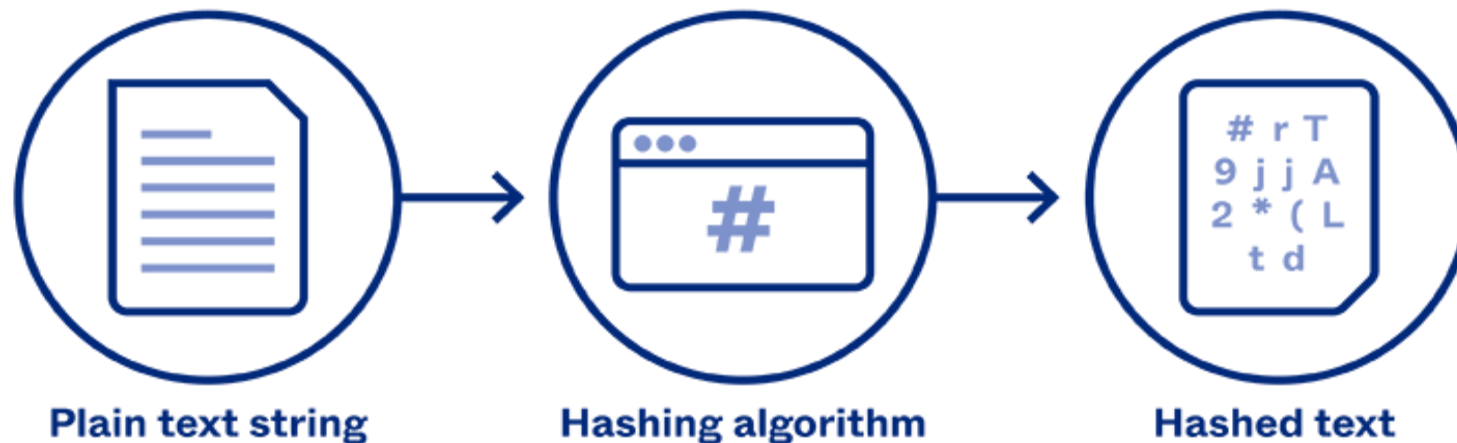
- 🔒 **Szyfrowanie** – ukrycie treści wiadomości
- 🔑 **Hasła i uwierzytelnianie** – dostęp tylko dla uprawnionych
- 📊 **Haszowanie** – wykrywanie zmian w danych
- ✍️ **Podpis cyfrowy** – potwierdzenie tożsamości nadawcy
- 💾 **Kopie zapasowe** – dane nie znikną po awarii



CO TO JEST HASZOWANIE?

Haszowanie to przekształcenie danych (np. hasła) w krótki, nieodwracalny ciąg znaków.

-  Z jednego hasła → zawsze ten sam hash
-  Mała zmiana → zupełnie inny wynik
-  Nie da się „cofnąć” hasha do oryginału - ale można próbować je zgadnąć



DLACZEGO HASŁA MUSZĄ BYĆ HASZOWANE?



✗ Jeśli ktoś ukradnie bazę z hasłami w formie jawnej – zna Twoje dane

✓ Jeśli hasła są haszowane – zobaczy tylko ich skróty

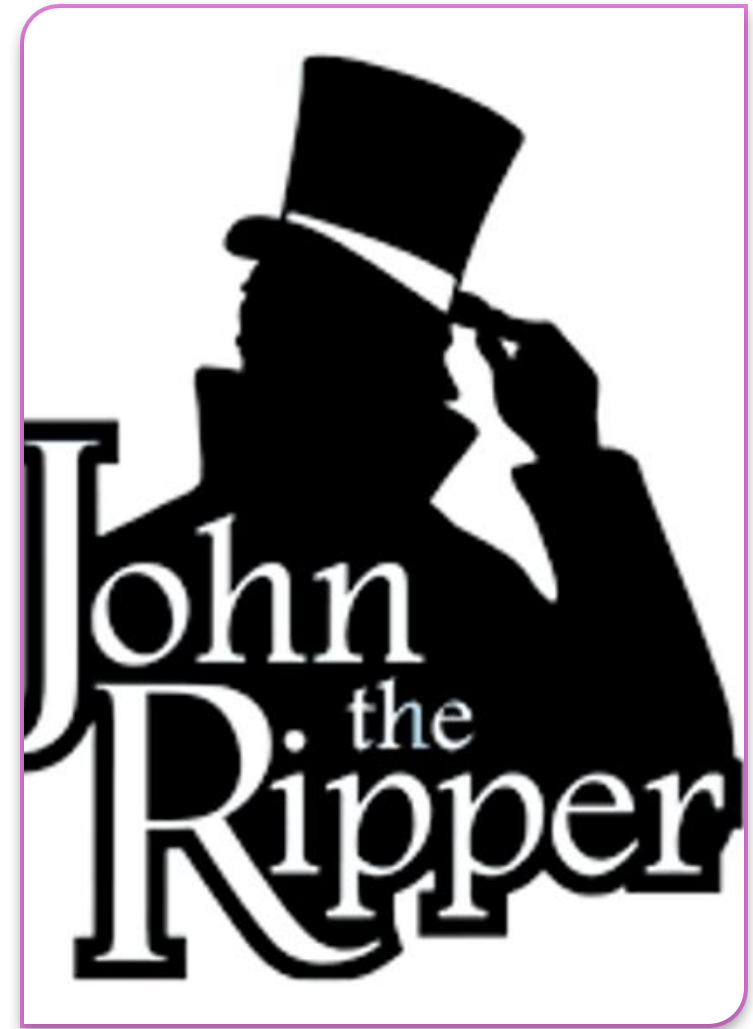
🔍 Ale uwaga! Słabe hasła da się odgadnąć porównując hashe

JAK ŁAMIE SIĘ HASŁA MIMO HASZOWANIA?

- 🏠 Atak słownikowy – próba zgadywania haseł z listy (np. `rockyou.txt`)
- 💣 Brute force – sprawdzanie wszystkich możliwych kombinacji
- 🌈 Tęczowe tablice – gotowe bazy hashów popularnych haseł
- ⚠️ Kolizje – dwa różne hasła dają ten sam hash (w słabych algorytmach, np. MD5)

ŁAMANIE HASŁA Z JOHN THE RIPPER

John the Ripper – program służący do łamania haseł. Początkowo stworzony dla systemu operacyjnego UNIX, aktualnie uruchamia się na piętnastu różnych platformach. Jest to jeden z najpopularniejszych programów do łamania oraz testowania haseł. Formaty, które obsługuje to DES, RSA, MD4 i MD5, Kerberos AFS oraz hasze Windows LM. Dodatkowe moduły umożliwiają obsługę LDAP, MySQL i podobnych.



WYNIK ŁAMANIA HASŁA

Plik hashes.txt zawiera hash hasła `password` zakodowany w algorytmie MD5

Uruchamiamy narzędzie **John the Ripper**, które ładuje słownik (`rockyou.txt`) zawierający miliony haseł z wycieków, porównuje każde słowo z hashem w pliku, rozpoznaje typ hasha jako **MD5**.

Hasło `password` zostaje złamane błyskawicznie – John dopasowuje hash do słowa z listy

Widzimy wynik: `?:password` co oznacza: „dla jednego wpisu z pliku hasłem było `password`”.

```
parallels@ubuntu-linux-22-04-desktop:~$ cat ~/hashes.txt
5f4dcc3b5aa765d61d8327deb882cf99
parallels@ubuntu-linux-22-04-desktop:~$ cd ~/john/run
./john --format=raw-md5 --wordlist=/home/parallels/rockyou.txt ~/hashes.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 ASIMD 4x2])
Cracked 1 password hash (is in ./john.pot), use "--show"
No password hashes left to crack (see FAQ)
parallels@ubuntu-linux-22-04-desktop:~/john/run$ ./john --show --format=raw-md5
~/hashes.txt
?:password

1 password hash cracked, 0 left
```

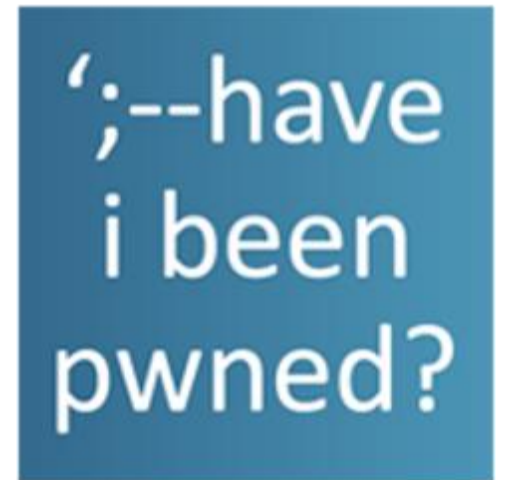
CO TO JEST I JAK DZIAŁA HAVE I BEEN PWNED?

Have I Been Pwned (HIBP) to publiczna baza danych wycieków danych, stworzona przez Troya Hunta.

Pozwala każdemu sprawdzić, czy jego e-mail lub hasło pojawiło się w znanych wyciekach (np. LinkedIn, Dropbox, Adobe...).

Oferuje:

- Wyszukiwanie po e-mailu
- Sprawdzanie hashy haseł (SHA-1)
- System "k-Anonymity" — serwis nie zna Twojego hasła ani nie przechowuje e-maila wprost



SPRAWDZANIE DANYCH NA HIBP

Sprawdzanie adresu e-mail:

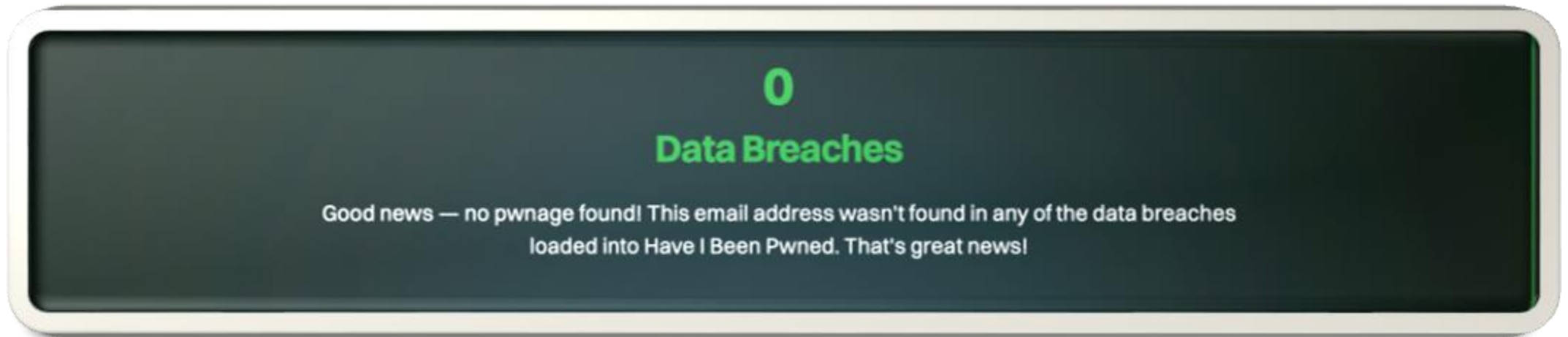
- Wejdź na: <https://haveibeenpwned.com/>
- Wpisz e-mail

Zobacz, w których wyciekach się pojawił

Sprawdzenie hasła:

- Wejdź na: <https://haveibeenpwned.com/Passwords>
- Wpisz np. 12345678

Zobacz, ile razy to hasło zostało znalezione



JAK DŁUGO ZAJMUJE ZŁAMANIE TWOJEGO HASŁA?

Hardware: 12 x RTX 5090 Password hash: bcrypt (10)					
Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	57 minutes	2 hours	4 hours
6	Instantly	46 minutes	2 days	6 days	2 weeks
7	Instantly	20 hours	4 months	1 year	2 years
8	Instantly	3 weeks	15 years	62 years	164 years
9	2 hours	2 years	791 years	3k years	11k years
10	1 day	40 years	41k years	238k years	803k years
11	1 weeks	1k years	2m years	14m years	56m years
12	3 months	27k years	111m years	917m years	3bn years
13	3 years	705k years	5bn years	56bn years	275bn years
14	28 years	18m years	300bn years	3tn years	19tn years
15	284 years	477m years	15tn years	218tn years	1qd years
16	2k years	12bn years	812tn years	13qd years	94qd years
17	28k years	322bn years	42qd years	840qd years	6qn years
18	284k years	8tn years	2qn years	52qn years	463qn years

Tabela pokazuje czas łamania haseł w zależności od:

- długości hasła (4-18 znaków)
- rodzaju znaków (cyfry, litery, symbole)

Testy wykonano z użyciem bcrypt (rounds: 10) na 12 kartach RTX 5090 – potężnej konfiguracji dostępnej dla zorganizowanych grup cyberprzestępczych.

Ale...

CO JEŚLI MOJE HASŁO ZNALAZŁO SIĘ W WYCIEKU?

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	Instantly	Instantly	Instantly
8	Instantly	Instantly	Instantly	Instantly	Instantly
9	Instantly	Instantly	Instantly	Instantly	Instantly
10	Instantly	Instantly	Instantly	Instantly	Instantly
11	Instantly	Instantly	Instantly	Instantly	Instantly
12	Instantly	Instantly	Instantly	Instantly	Instantly
13	Instantly	Instantly	Instantly	Instantly	Instantly
14	Instantly	Instantly	Instantly	Instantly	Instantly
15	Instantly	Instantly	Instantly	Instantly	Instantly
16	Instantly	Instantly	Instantly	Instantly	Instantly
17	Instantly	Instantly	Instantly	Instantly	Instantly
18	Instantly	Instantly	Instantly	Instantly	Instantly

Nawet najdłuższe hasło **nie chroni** Cię, jeśli było częścią wycieku danych.


Jeśli Twoje hasło:

- było proste,
- powtórzyło się w różnych serwisach,
- lub zostało ujawnione w wycieku...


...to atakujący **ma je już w swojej bazie** i może je rozpoznać **natychmiast** – bez łamania.

Wtedy czas łamania to praktycznie **0 sekund**

GDY TWOJE HASŁO WYCIEKNIE – CO SIĘ Z NIM DZIEJE?




 Hasła to towar – sprzedawane na forach, darknetowych giełdach i grupach Telegram

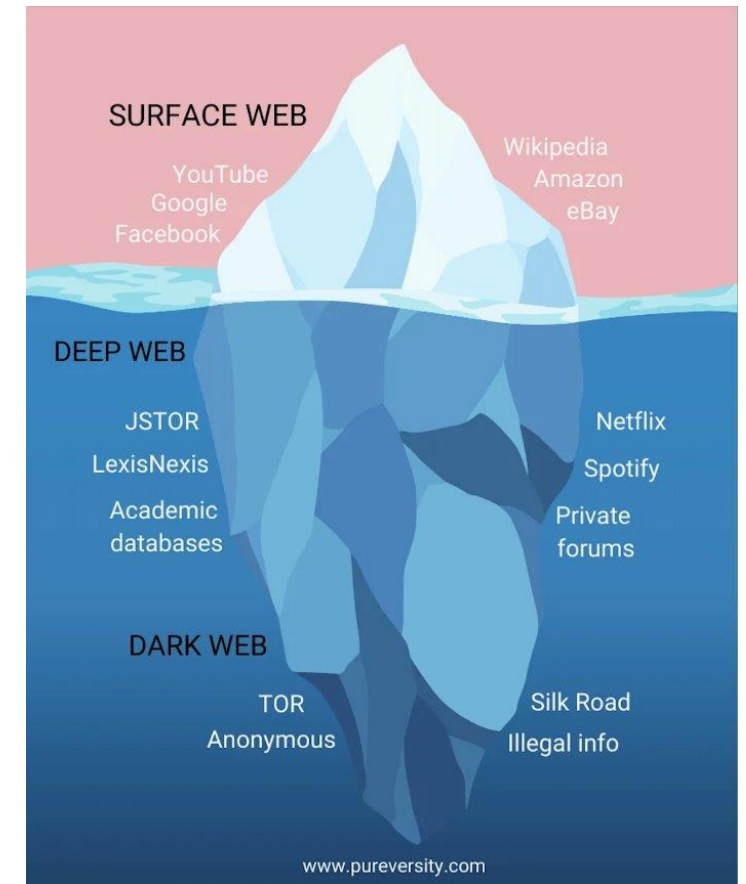
 Zestawy danych zawierają: e-mail, login, hasło, lokalizację, numer telefonu

 Kupujący to spamerzy, oszuści, boty logujące się automatycznie

 Dane są używane w atakach: credential stuffing, phishing, kradzież tożsamości

GDZIE TE DANE TRAFIAJĄ?

 Surface web	Normalny internet, wyszukiwalny w Google (np. Allegro, Facebook)
 Deep web	Ukryte części sieci (np. skrzynka pocztowa, wewnętrzne systemy firm)
 Dark web	Anonimowa sieć – dostęp tylko przez TOR. Tu handluje się danymi i zleceniami przestępstw.



ILE WARTĘ SĄ TWOJE DANE? – DARK WEB PRICE INDEX 2024



- 💳 Dane z karty kredytowej (z limitem do 5 000 USD): \$120
- 📺 Konto Netflix: \$25
- 📺 Konto HBO: \$4
- 👤 Selfie z dowodem osobistym: \$120
- 📁 Pakiet 720 000 danych użytkowników: \$17 000 000
- 🌐 Łączny koszt cyberprzestępczości dla świata: \$445 miliardów rocznie

JAK TWORZYĆ SILNE HASŁA?

Długość ma znaczenie -
Twoje hasło powinno
mieć co najmniej 12
znaków.

Używaj różnych typów
znaków - mieszaj małe i
wielkie litery, cyfry oraz
znaki specjalne
(!@#\$%^&*).

Unikaj przewidywalnych
hasel - „123456”,
„password” lub „qwerty”
są łatwe do złamania.

Nie używaj swoich danych
osobowych - imię,
nazwisko, data urodzenia
to złe pomysły.







Nie używaj jednego hasła
na wielu stronach - w
przypadku wycieku,
możesz stracić dostęp do
wielu kont.

Zastanów się nad użyciem
menedżera haseł -
zapamięta on Twoje hasła
i wygeneruje silne
kombinacje.

Nie udostępniaj swojego
hasła nikomu - nigdy,
nawet znajomym.

SPRAWDŹ SIŁĘ HASŁA!



Co robi aplikacja?


-  Analizuje siłę wpisanego hasła i podaje ocenę jego złożoności
-  Pokazuje czas potrzebny do złamania hasła (na podstawie tabeli Hive Systems 2025)
-  Sprawdza, czy hasło pojawiło się w znanych wyciekach danych korzystając z Have I Been Pwned
-  Podpowiada, jak poprawić swoje hasło i jak tworzyć silniejsze
-  Nie wysyła żadnych haseł, a jedynie pierwsze 5 znaków ich skrótów (SHA-1)
-  Pozwala wygenerować nowe, silne hasło jednym kliknięciem

<https://cybersecurity789.github.io/>

Analiza Bezpieczeństwa Hasła

Wpisz hasło, aby sprawdzić jego siłę:

 Hasło nie występuje w znanych wyciekach.

Siła hasła: Średnie

Czas złamania: 17 lat

[Wygeneruj silne hasło](#)

ŹRÓDŁA

- [1] John the Ripper - https://pl.wikipedia.org/wiki/John_the_Ripper
- [2] Co to jest phishing? Przykłady + jak się bronić przed atakiem phishingowym
<https://kwestiabezpieczenstwa.pl/phishing/>
- [3] Are Your Passwords in the Green? <https://www.hivesystems.com/blog/are-your-passwords-in-the-green>
- [4] Hashing Algorithm Overview: Types, Methodologies & Usage <https://www.okta.com/uk/identity-101/hashing-algorithms/>
- [5] Delete Yourself, Part 2: Your Personal Data on the Dark Web
<https://www.wsj.com/tech/personal-tech/data-breach-dark-web-protection-6972f3a6>
- [6] How much is your data worth on the dark web?
<https://www.wipfli.com/insights/articles/dark-web-price-index>
- [7] How Hackers Steal Passwords: 5 Attack Methods Explained:
<https://www.youtube.com/watch?v=vKPGZHoHX8k>