1110111011011

1001100

110011001100

10101010101010

00011001001

Sposoby łamania haseł

Kali Linux – Password Cracking

Hacking i Cyberbezpieczeństwo | Giganci Programowania

Opracowanie: Michał Suchoń

Przypomnienie

1. Która metoda rekonesansu (Information Gathering) jest bardziej ryzykowna – **pasywna czy aktywna?**

2. Czym różni się hashowanie od szyfrowania?

3. Czy OSINT to legalna metoda pozyskiwania informacji?

Przypomnienie

1. Która metoda rekonesansu (Information Gathering) jest bardziej ryzykowna – **pasywna czy aktywna?**

   Metoda aktywna wiąże się z dużo większym ryzykiem, ponieważ opiera się o bezpośredniej próbie nawiązania połączenia (w sposób niejawny) z urządzeniem ofiary. Z tego względu, istnieje zagrożenie wykrycia. W metodzie pasywnej używa się zewnętrznych narzędzi, dzięki czemu szanse na wykrycie atakującego jest niemal zerowe.

2. Czym różni się hashowanie od szyfrowania?

3. Czy OSINT to legalna metoda pozyskiwania informacji?

Przypomnienie

1. Która metoda rekonesansu (Information Gathering) jest bardziej ryzykowna – **pasywna czy aktywna?**

   Metoda aktywna wiąże się z dużo większym ryzykiem, ponieważ opiera się o bezpośredniej próbie nawiązania połączenia (w sposób niejawny) z urządzeniem ofiary. Z tego względu, istnieje zagrożenie wykrycia. W metodzie pasywnej używa się zewnętrznych narzędzi, dzięki czemu szanse na wykrycie atakującego jest niemal zerowe.

2. Czym różni się hashowanie od szyfrowania?

   Szyfrowanie jest procesem odwracalnym (szyfrowanie i deszyfrowanie) – hashowanie nie. Odczytanie informacji z hasha, np. zbadanie poprawności hasła, polega na porównaniu dwóch ciągów zahashowanych tym samym algorytmem (RSA, SHA1 etc.)

3. Czy OSINT to legalna metoda pozyskiwania informacji?

Przypomnienie

1. Która metoda rekonesansu (Information Gathering) jest bardziej ryzykowna – **pasywna czy aktywna?**

   Metoda aktywna wiąże się z dużo większym ryzykiem, ponieważ opiera się o bezpośredniej próbie nawiązania połączenia (w sposób niejawny) z urządzeniem ofiary. Z tego względu, istnieje zagrożenie wykrycia. W metodzie pasywnej używa się zewnętrznych narzędzi, dzięki czemu szanse na wykrycie atakującego jest niemal zerowe.

2. Czym różni się hashowanie od szyfrowania?

   Szyfrowanie jest procesem odwracalnym (szyfrowanie i deszyfrowanie) – hashowanie nie. Odczytanie informacji z hasha, np. zbadanie poprawności hasła, polega na porównaniu dwóch ciągów zahashowanych tym samym algorytmem (RSA, SHA1 etc.)

3. Czy OSINT to legalna metoda pozyskiwania informacji?

   OSINT (*OpenSource Intelligence*) zakłada korzystanie z czysto otwartych źródeł, co jest całkowicie legalne (nikt nam nie zabroni korzystać z internetu by czegoś się dowiedzieć!)

Jak działa hashowanie?

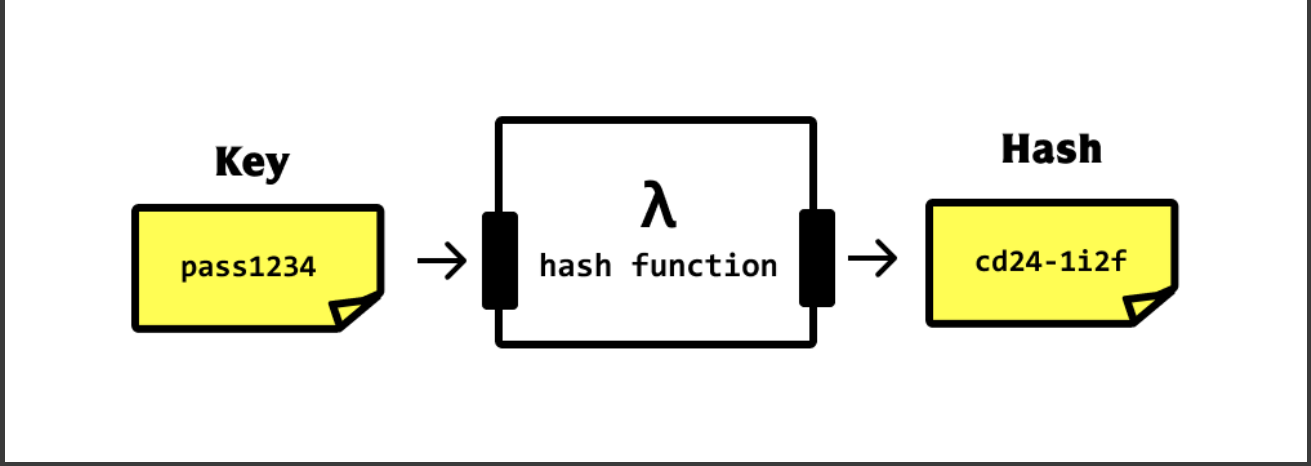
Hashowanie

Jest obecnie jednym z najlepszych metod zabezpieczania haseł. Hash tworzony jest za pomocą tzw. funkcji haszującej (skrótu / mieszającej)

Funkcja haszująca

(skrótu, mieszająca)

Przyporządkowuje dowolnej wartości o różnej długości (nawet bardzo dużej), krótką *quasi-losową* o stałym rozmiarze, niespecyficzna. Najpopularniejsze funkcje haszujące to m.in. SHA1, SHA2, SHA256, SHA512, MD5 (ostatnia niezalecana – dawno złamana).



szybkość łamania – MD5

CPU
procesor

ZALEŻY OD SZYBKOŚCI PROCESORA, TJ. JEGO PARAMETRÓW:

- **ILOŚĆ RDZENI** (*równoległe obliczenia na kilka rdzeni jednocześnie*)
- **TAKTOWANIE PROCESORA** (*ilość instrukcji na jednostkę czasu*)
- **OBSŁUGA SSE2** *(kilka instrukcji na jeden takt zegara)*

UWAGA! GENERACJA NIE MA WIĘKSZEGO ZNACZENIA OBECNIE (JEŚLI OBSŁUGUJE SSE2)

Istotne jest także, aby algorytm łamiący hash został odpowiednio optymalizowany. **Im lepsza optymalizacja kodu, tym krótszy czas wykonania.**

GPU
karta graficzna

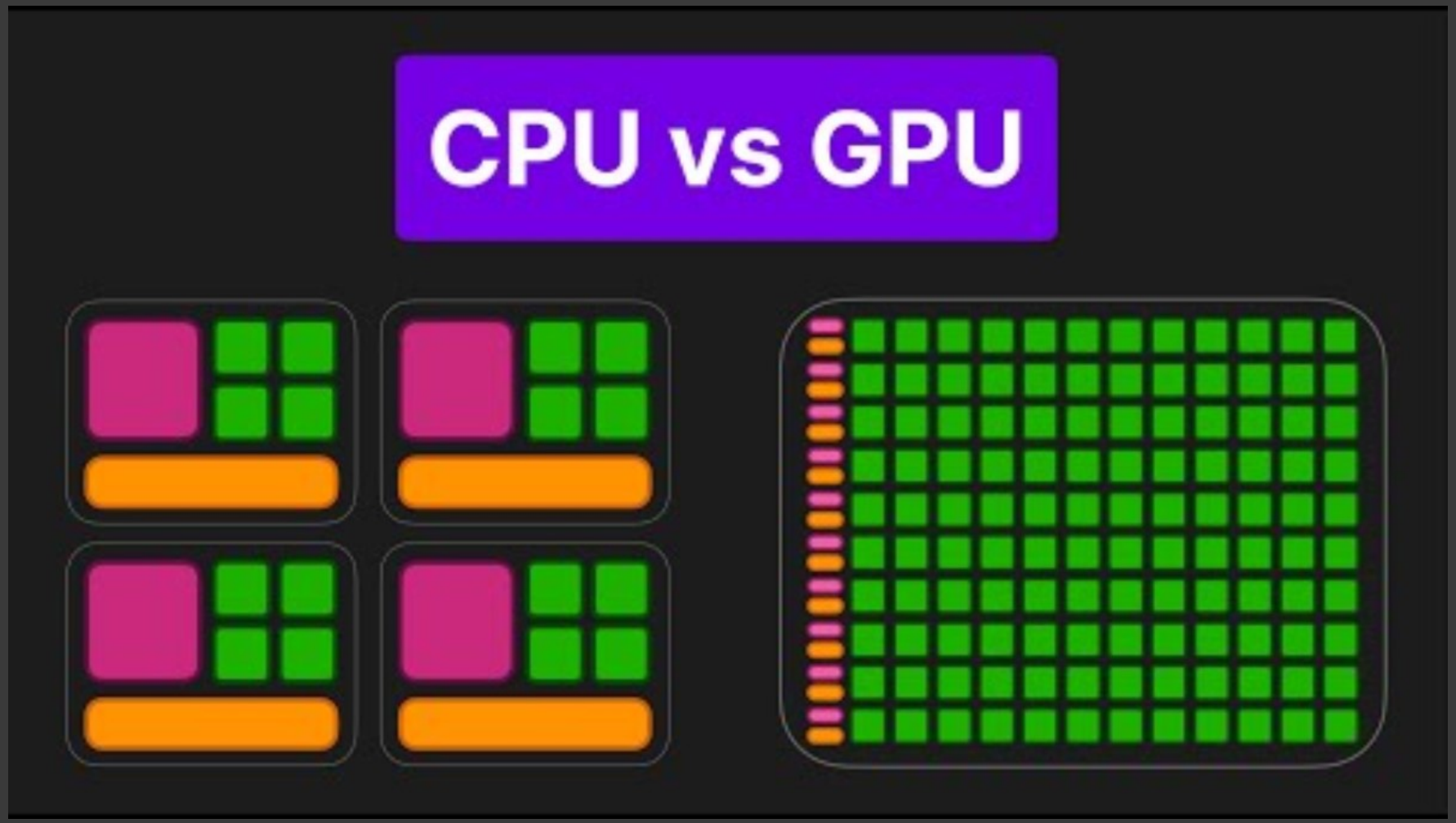
DOBRE CRACKERY WYKORZYSTUJĄ NOWOCZESNE KARTY GRAFICZNE (NVIDIA – CUDA, AMD Radeon – Stream). Dzięki temu, możliwy jest **skokowy wzrost wydajności w porównaniu do odpowiedników, wykorzystujących CPU.**

Nowoczesne GPU posiadają wiele ALU (*Arithmetic Logic Unit*) bądź tzw. **procesory strumieniowe** (*stream procesor*) – **jednostki mogące równolegle realizować pewne operacje matematyczne na liczbach całkowitych** (obecne GPU posiadają nawet 3000 ALU) -> **ŁAMANIE POJEDYNCZEGO HASŁA JEST ZRÓWNOLEGLONE NA PROCESORY STRUMIENIOWE, CZYLI JEŚLI MAMY 3000 ALU TO TAK, JAKBYŚMY POSIADALI CPU O 3000 RDZENIACH**

JAK WYLICZYĆ SZYBKOŚĆ?

Dla procesora Radeon HD 5970 to ok. **8.5 mld hashy na sekundę** (Szybciej niż Cain&Abel na CPU). **Przyrost w porównaniu GPU do CPU choć nie jest oszałamiający (50-100 razy), lecz nadal spory.**

Architektura CPU vs GPU



https://www.youtube.com/watch?v=Axd50ew4pco

Kolizja funkcji skrótu (H)

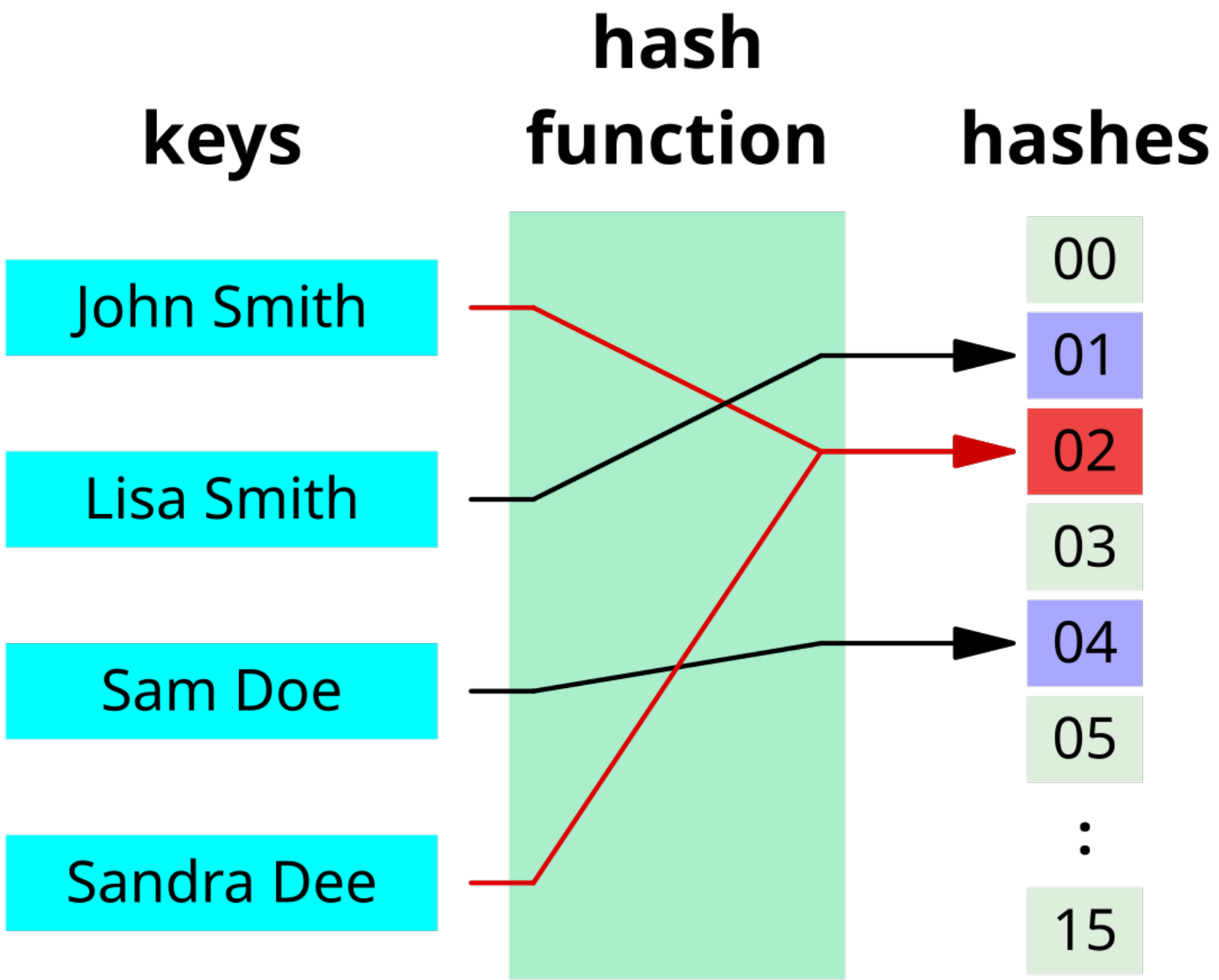
Są to takie dwie wiadomości (np. m_1 i m_2), które zwracają **ten sam hash, np.:**

- **dwóch użytkowników, posiadających ten sam hash hasła do swoich kont**
- **przy cyfrowym podpisie dokumentów, jeśli oba dokumenty posiadają ten sam hash, to można w ten sposób podrobić taki podpis na innym dokumencie.**

JAK UNIKNĄĆ KOLIZJI FUNKCJI SKRÓTU?

Najlepiej, aby stosować obecnie zalecane i silne funkcje skrótu, jak. Np.. **SHA-256/ SHA-512 czy SHA-3.** Warto także stosować skomplikowane hasła (słabo podatne na prawdopodobieństwo podania takiego samego przez kilka osób) bądź stosować dodatkowe zabezpieczenia hashy, jak np. **sól** (salt) – dane losowe, dodawane do hasła przy stosowaniu funkcji skrótu.

- ✓ ***Second preimage resistance*** *-> takie ciągi* m_1 *i* m_2*, że* $H(m_1) = H(m_2)$ *, gdzie H to funkcje skrótu*
- ✓ ***Preimage resistance*** *-> taki hash (h) ciągu m, że H(m) = h*


keys
hash function
hashes
John Smith
Lisa Smith
Sam Doe
Sandra Dee
00
01
02
03
04
05
:
15

Przypomnienie – metody łamania haseł

ALGORYTM SIŁOWY (BRUTE FORCE)

metoda sprawdzania wszystkich możliwych kombinacji znaków w celu znalezienia hasła

ALGORYTM SŁOWNIKOWY (DICTIONARY)

metoda sprawdzania kombinacji haseł za pomocą podzbiorów haseł, pochodzących np. z wycieków baz danych

NARZĘDZIA DO ŁAMANIA HASEŁ W KALI LINUX ZNAJDZIEMY W KATEGORII „PASSWORD ATTACKS”

ĆWICZENIE 1 | ŁAMANIE HASEŁ

Johnny The Riddle

POZWALA NA ZŁAMANIE HASŁA ZA POMOCĄ ATAKU BRUTE-FORCE BĄDŹ DICTIONARY

1. W terminalu zainstaluj pakiet **johnny**:
   - sudo apt-get update && sudo apt-get upgrade
   - sudo apt-get install johnny

2. Tworzymy nowego użytkownika, wraz z podaniem hasła:
   - useradd *{nazwa usera}*
   - passwd *{nazwa usera}* i podajemy hasło z potwórzeniem

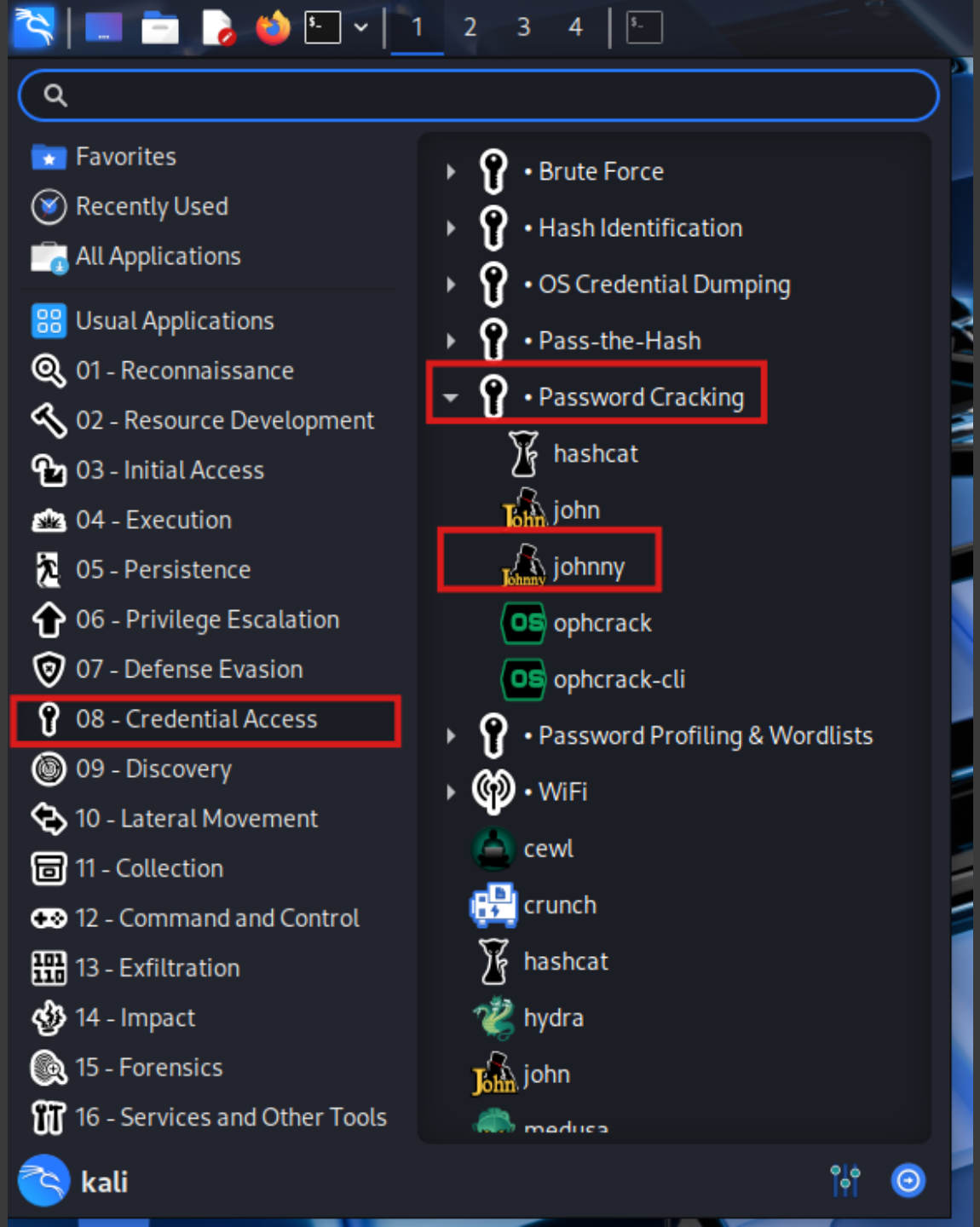
3. Informacje na temat uprawnień oraz haseł do kont (ich hashy), znajdziemy w:
   - **UPRAWNIENIA:** /etc/passwd
   - **HASHE:** /etc/shadow

4. Podajemy w terminalu „johnny”, aby uruchomić program. Spróbujemy złamać hasła podane w pliku *shadow*. **ZE WZGLĘDU NA TO, ŻE METODA BRUTE FORCE BYWA CZASOCHŁONNA, SKORZYSTAMY Z METODY SŁOWNIKOWEJ** (gotowe słowniki znajdziemy w katalogu **/usr/share/wordlists**)

Krok 1:

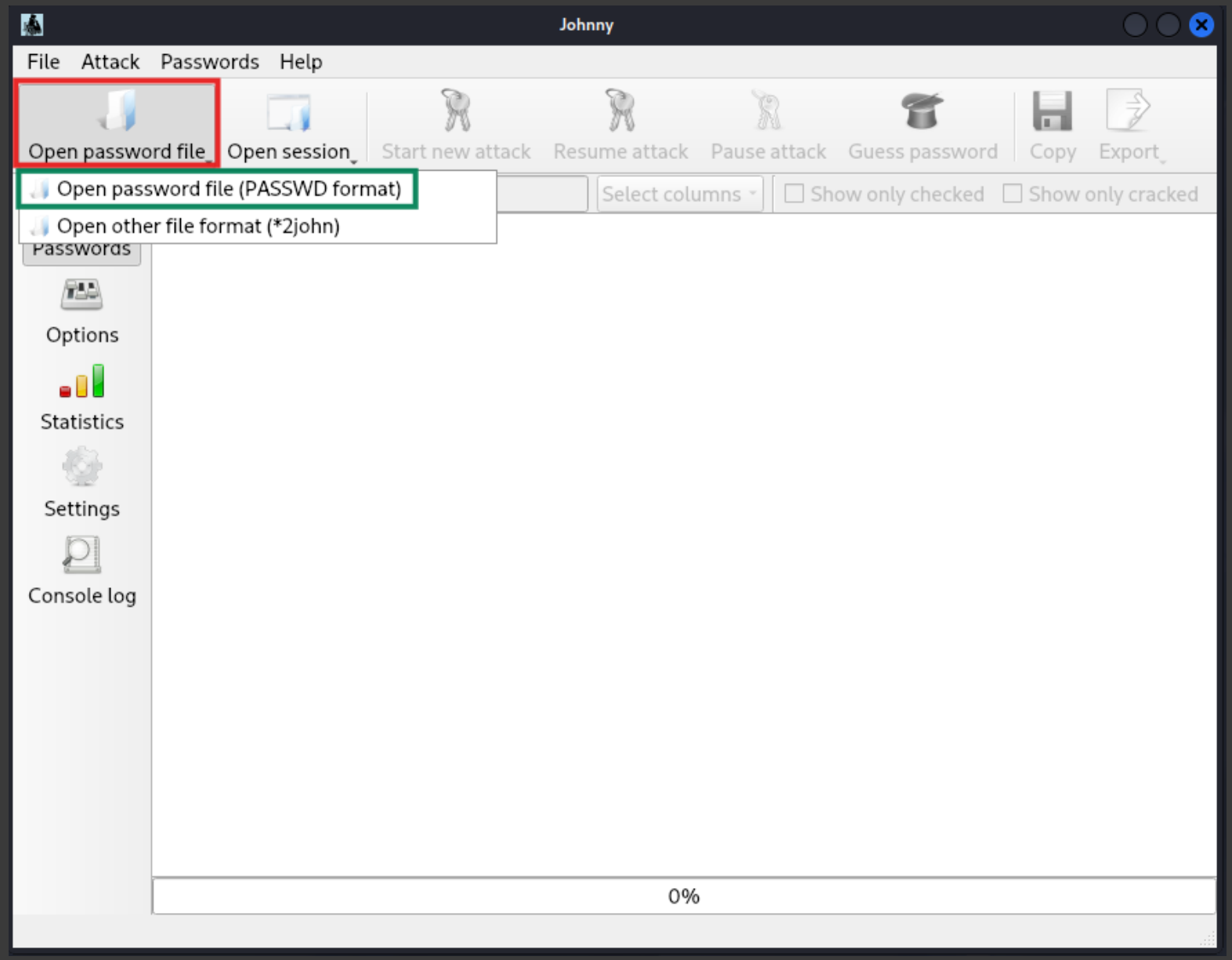
Lub polecenie w terminalu: **sudo johnny** (ważne, aby uruchomić z poziomu roota!)

UWAGA! URUCHAMIAJĄC PROGRAM PRZEZ INTERFEJS JAK OBOK MOŻNA WYŁĄCZNIE BĘDĄC NA KONCIE ROOTA!



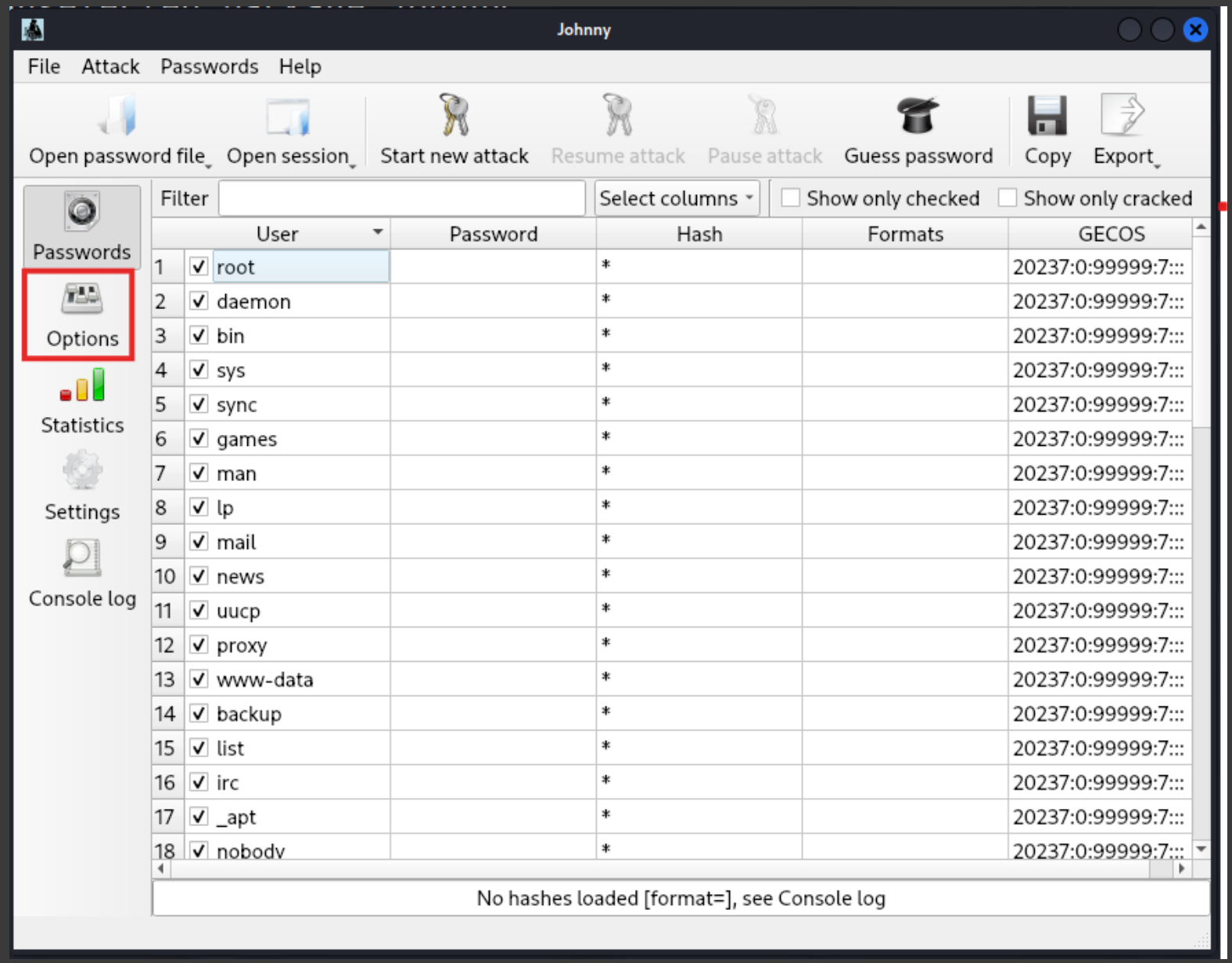
Krok 2:

Wczytujemy plik **shadow** z katalogu /etc/



Krok 3:

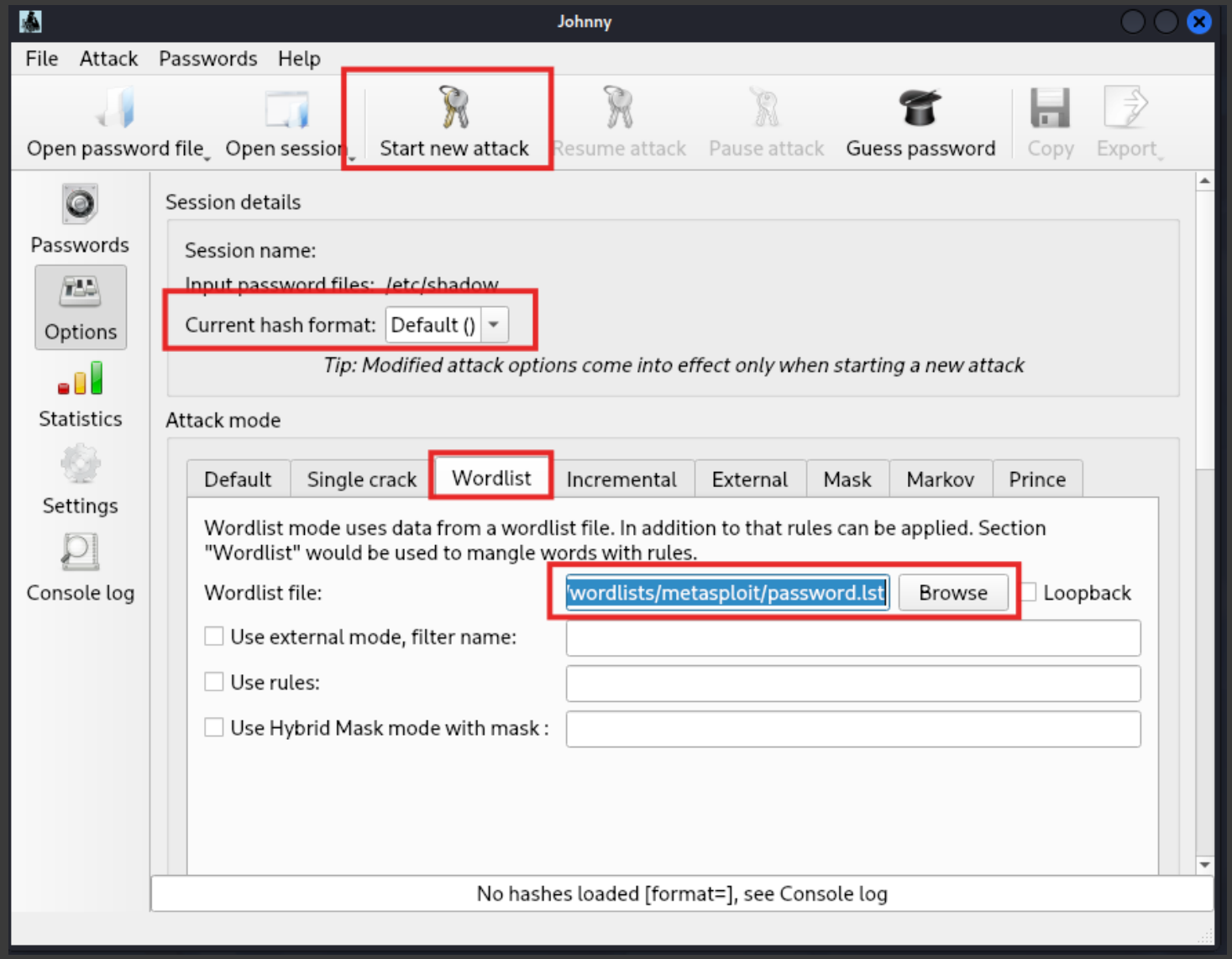
Przechodzimy do zakładki „Options” oraz „Wordlist” aby wczytać słownik (z katalogu **/usr/share/wordlists/metasploit/password.lst**), używając opcji „**Browse**”



Krok 4:

Po wczytaniu wordlisty, w *Current hash format* wybieramy **crypt** klikamy **Start new attack.** Czekamy na wynik

(zobaczymy je w sekcji *Passwords*)



ĆWICZENIE 2 | RARCRACK

RarCrack NARZĘDZIE DO PRZEPROWADZANIA SŁOWNIKOWYCH ATAKÓW

1. Szukamy w internecie słownik (najlepiej jakiś polski) dla konkretnego algorytmu bądź tworzymy plik o nazwie **plik.txt**, który pakujemy za pomocą 7zip'a i próbujemy znaleźć hasło. My skorzystamy z tej drugiej opcji (zip).

2. Instalujemy rarcrack: ***sudo apt-get install rarcrack***
3. Przechodzimy do Pulpitu i tworzymy folder *archiwum*, w którym tworzymy plik **plik.txt**:
   1. **cd Desktop**
   2. **mkdir archiwum**
   3. **cd archiwum**
   4. **touch plik.txt**

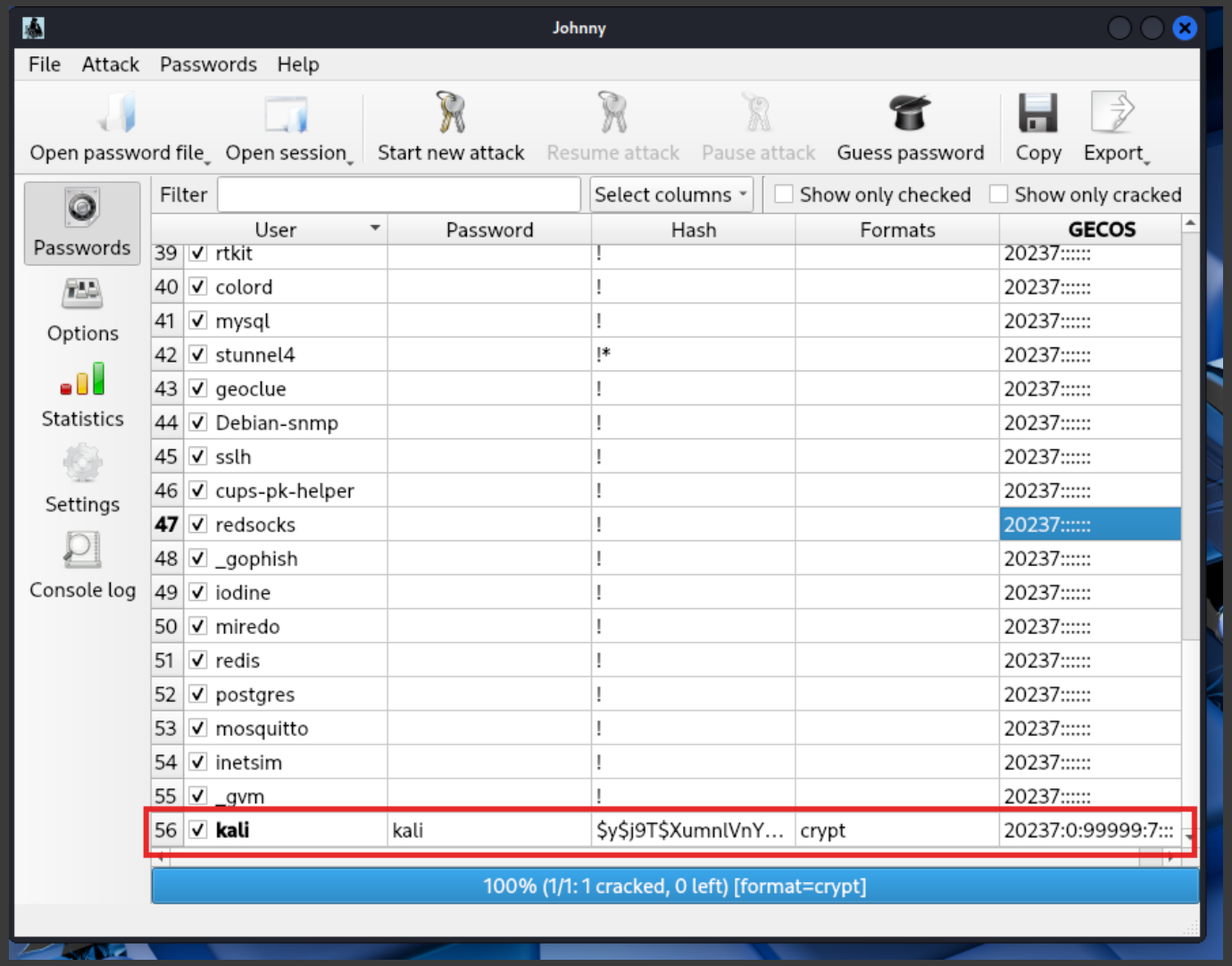
   (otwieramy np. za pomocą nano i podajemy hasło lub od razu: ***echo {hasło} > plik.txt***

ĆWICZENIE 2 | RARCRACK

RarCrack NARZĘDZIE DO PRZEPROWADZANIA SŁOWNIKOWYCH ATAKÓW

1. Pakujemy plik do archiwum: ***7z a –p password –mhe dane.7z plik.txt*** *(archiwum będzie opatrzone hasłem „password”)*

1. Uruchamiamy rarcrack: ***rarcrack dane.7z ––threads 32 ––type 7z***



Udało się! Tylko to konto ma aktywnie ustawione hasło, dlatego dla pozostałych kont komórki w kolumnie „Password” pozostają puste.

```
Probing: '7V8' [83 pwds/sec]
Probing: '7Z7' [82 pwds/sec]
Probing: '834' [81 pwds/sec]
Probing: '877' [83 pwds/sec]
Probing: '8aZ' [80 pwds/sec]
Probing: '8eW' [81 pwds/sec]
Probing: '8iV' [82 pwds/sec]
Probing: '8mZ' [84 pwds/sec]
Probing: '8qT' [80 pwds/sec]
Probing: '8uP' [81 pwds/sec]
Probing: '8yS' [83 pwds/sec]
Probing: '8CP' [81 pwds/sec]
Probing: '8Gz' [77 pwds/sec]
Probing: '8Ku' [81 pwds/sec]
Probing: '8NH' [66 pwds/sec]
Probing: '8Rc' [72 pwds/sec]
Probing: '8UV' [77 pwds/sec]
Probing: '8YG' [77 pwds/sec]
Probing: '92y' [80 pwds/sec]
Probing: '96y' [82 pwds/sec]
Probing: '9ad' [75 pwds/sec]
Probing: '9dY' [77 pwds/sec]
```

Podsumowanie

1. Jakie są metody łamania haseł?
2. Jakie musi być hasło, aby było trudne do złamania (lub nie do złamania w rozsądnym czasie)?

Polecam!

ŹRÓDŁO:
https://www.youtube.com/watch?v=8ZtInClXe1Q

Polecam!

ŹRÓDŁO:
https://www.youtube.com/watch?v=jsraR-el8_o