Zadanie 2 - Łamanie haseł (met.słownikowa) 1/2

Środowisko: Kali Linux

Dla podanych niżej hashy określ typ wykorzystanego algorytmu hashującego, a następnie złam hasło metodą słownikową.

Hasła pochodzą ze słownika rockyou-50.

1. 9fd8301ac24fb88e65d9d7cd1dd1b1ec

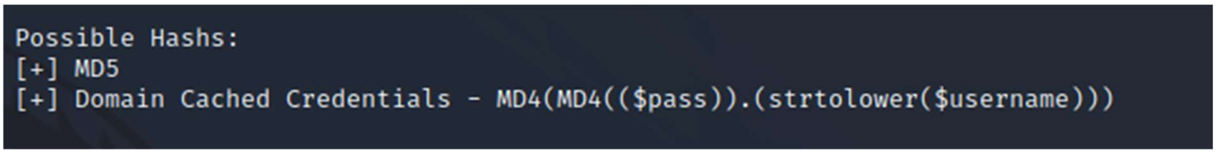
2. 7f9a6871b86f40c330132c4fc42cda59

3. 6104df369888589d6dbea304b59a32d4

4. 276f8db0b86edaa7fc805516c852c889

5. 04dac8afe0ca501587bad66f6b5ce5ad

Typ dla wszystkich: MD5

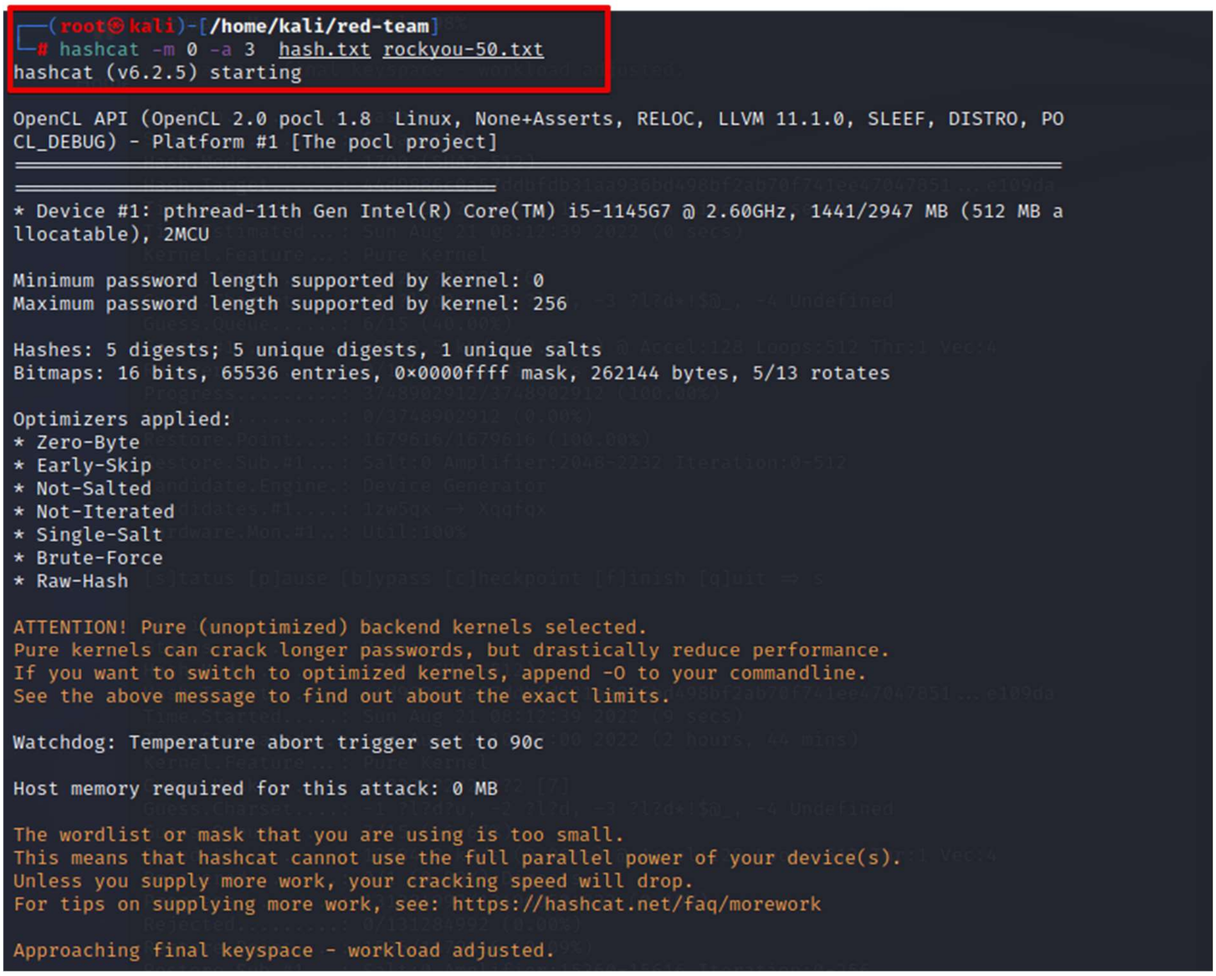


```
Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))
```

Komenda:

hashcat -m 0 -a 0 hash.txt rockyou-50.txt

gdzie hash.txt to powyższe hashe



```
┌──(root㉿kali)-[/home/kali/red-team]
└─# hashcat -m 0 -a 3  hash.txt rockyou-50.txt
hashcat (v6.2.5) starting

OpenCL API (OpenCL 2.0 pocl 1.8  Linux, None+Asserts, RELOC, LLVM 11.1.0, SLEEF, DISTRO, PO
CL_DEBUG) - Platform #1 [The pocl project]
==========================================================================================
=========================================

* Device #1: pthread-11th Gen Intel(R) Core(TM) i5-1145G7 @ 2.60GHz, 1441/2947 MB (512 MB a
llocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 5 digests; 5 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Brute-Force
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.
```

Rozwiązanie:

9fd8301ac24fb88e65d9d7cd1dd1b1ec:**butterfly**

7f9a6871b86f40c330132c4fc42cda59:**tinkerbell**

6104df369888589d6dbea304b59a32d4:**blink182**

276f8db0b86edaa7fc805516c852c889:**baseball**

04dac8afe0ca501587bad66f6b5ce5ad:**hellokitty**

Zadanie 2 - Łamanie haseł (met.słownikowa) 2/2

Środowisko: Kali Linux

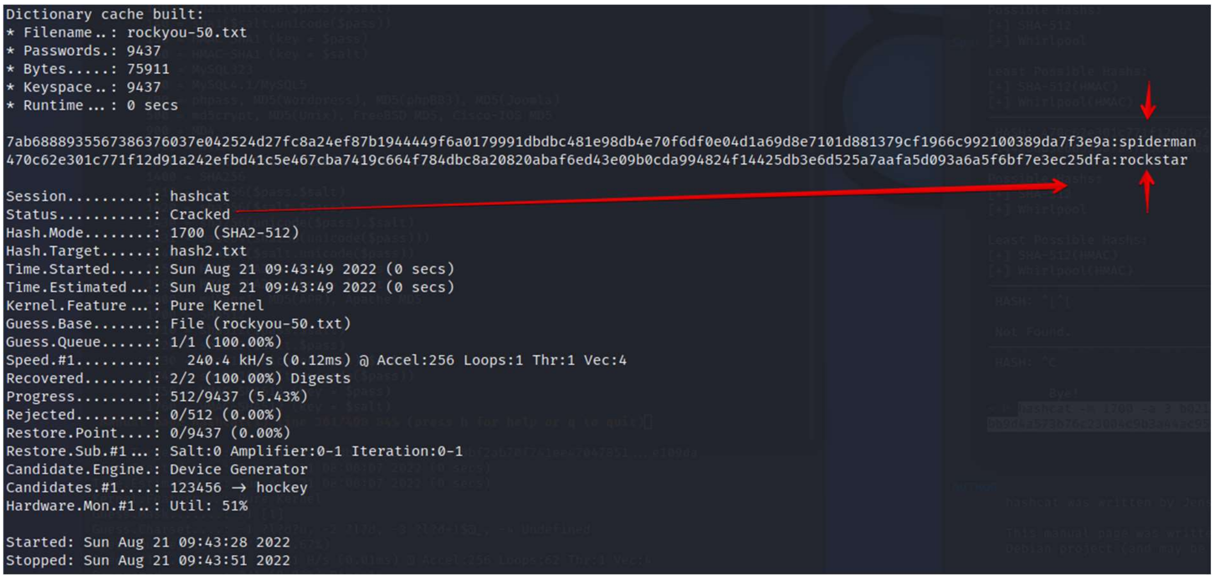
Dla podanych niżej hashy określ typ wykorzystanego algorytmu hashującego, a następnie złam hasło metodą słownikową.

Hasła pochodzą ze słownika rockyou-50.

1.
7ab6888935567386376037e042524d27fc8a24ef87b1944449f6a0179991dbdbc481e98db4e70f6df0e04d1a69d8e7101d881379cf1966c992100389da7f3e9a

2.
470c62e301c771f12d91a242efbd41c5e467cba7419c664f784dbc8a20820abaf6ed43e09b0cda994824f14425db3e6d525a7aafa5d093a6a5f6bf7e3ec25dfa

typy dla każdego: SHA-512

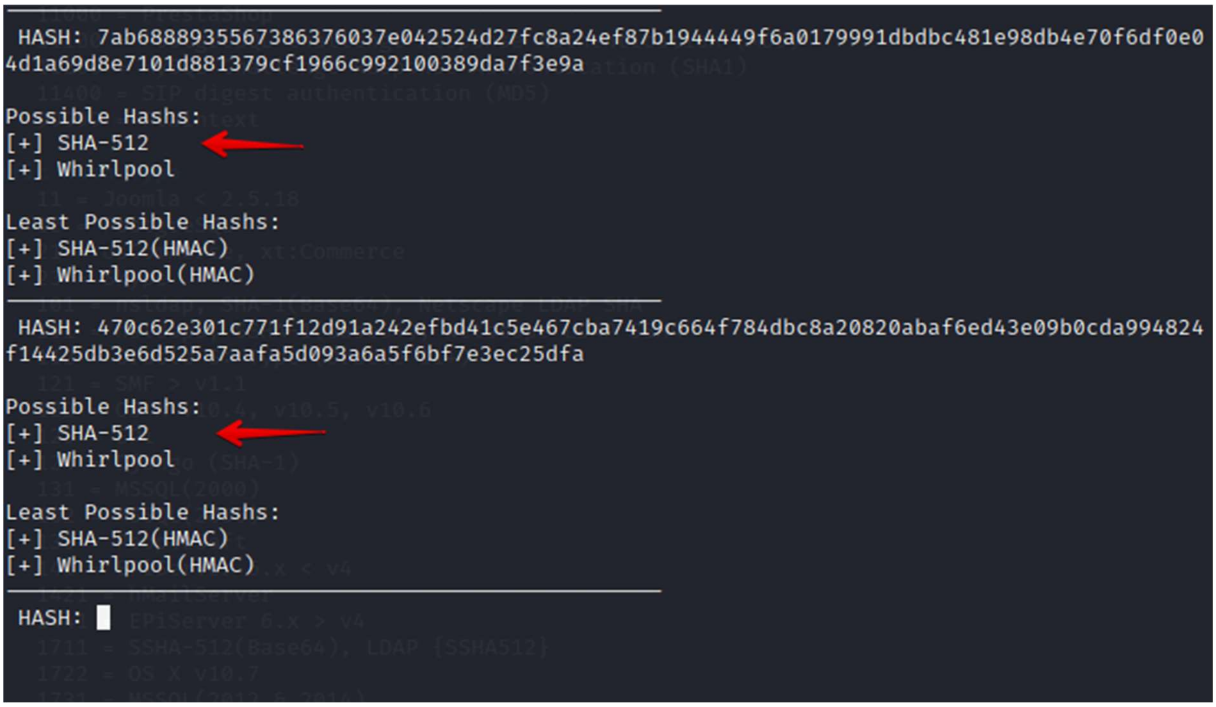


```
Dictionary cache built:
* Filename..: rockyou-50.txt
* Passwords.: 9437
* Bytes.....: 75911
* Keyspace..: 9437
* Runtime...: 0 secs

7ab6888935567386376037e042524d27fc8a24ef87b1944449f6a0179991dbdbc481e98db4e70f6df0e04d1a69d8e7101d881379cf1966c992100389da7f3e9a:spiderman
470c62e301c771f12d91a242efbd41c5e467cba7419c664f784dbc8a20820abaf6ed43e09b0cda994824f14425db3e6d525a7aafa5d093a6a5f6bf7e3ec25dfa:rockstar

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1700 (SHA2-512)
Hash.Target......: hash2.txt
Time.Started.....: Sun Aug 21 09:43:49 2022 (0 secs)
Time.Estimated...: Sun Aug 21 09:43:49 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (rockyou-50.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   240.4 kH/s (0.12ms) @ Accel:256 Loops:1 Thr:1 Vec:4
Recovered........: 2/2 (100.00%) Digests
Progress.........: 512/9437 (5.43%)
Rejected.........: 0/512 (0.00%)
Restore.Point....: 0/9437 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 → hockey
Hardware.Mon.#1..: Util: 51%

Started: Sun Aug 21 09:43:28 2022
Stopped: Sun Aug 21 09:43:51 2022
```



```
 --------------------------------------------------
 HASH: 7ab688893556738637603 7e042524d27fc8a24ef87b1944449f6a0179991dbdbc481e98db4e70f6df0e0
4d1a69d8e7101d881379cf1966c992100389da7f3e9a

Possible Hashs:
[+] SHA-512
[+] Whirlpool

Least Possible Hashs:
[+] SHA-512(HMAC)
[+] Whirlpool(HMAC)
 --------------------------------------------------
 HASH: 470c62e301c771f12d91a242efbd41c5e467cba7419c664f784dbc8a20820abaf6ed43e09b0cda994824
f14425db3e6d525a7aafa5d093a6a5f6bf7e3ec25dfa

Possible Hashs:
[+] SHA-512
[+] Whirlpool

Least Possible Hashs:
[+] SHA-512(HMAC)
[+] Whirlpool(HMAC)
 --------------------------------------------------
 HASH: █
```

komenda: hashcat -m 1700 -a 0 hash2.txt rockyou-50.txt

Rozwiązanie:

7ab6888935567386376037e042524d27fc8a24ef87b1944449f6a0179991dbdbc481e98db4e70f6df0e04d1a69d8e7101d881379cf1966c992100389da7f3e9a:**spiderman**

470c62e301c771f12d91a242efbd41c5e467cba7419c664f784dbc8a20820abaf6ed43e09b0cda994824f14425db3e6d525a7aafa5d093a6a5f6bf7e3ec25dfa:**rockstar**