

CRACKING DELLE PASSWORD CON GLI HASH

```
(kali@kali)-[~/Desktop]
$ hashcat -m 0 -a 0 hash.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 17.0.6, SLE
EF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

=====

* Device #1: cpu-penryn-Intel(R) Core(TM) i7-7700K CPU @ 4.20GHz, 2193/4451 MB (1024 MB al
locatable), 3MCU

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

Hashes: 5 digests; 4 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* 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

Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime ...: 1 sec

5f4dcc3b5aa765d61d8327deb882cf99:password
e99a18c428cb38d5f260853678922e03:abc123
0d107d09f5bbe40cade3de5c71e9e9b7:letmein
8d3533d75ae2c3966d7e0d4fcc69216b:charley

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 0 (MD5)
Hash.Target.....: hash.txt
Time.Started....: Wed Jul 3 22:49:23 2024 (0 secs)
Time.Estimated...: Wed Jul 3 22:49:23 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 54153 H/s (0.13ms) @ Accel:512 Loops:1 Thr:1 Vec:4
Recovered.....: 4/4 (100.00%) Digests (total), 4/4 (100.00%) Digests (new)
Progress.....: 3072/14344385 (0.02%)
Rejected.....: 0/3072 (0.00%)
Restore.Point....: 1536/14344385 (0.01%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: clover -> dangerous
Hardware.Mon.#1..: Util: 34%

Started: Wed Jul 3 22:49:10 2024
Stopped: Wed Jul 3 22:49:23 2024
```

Ho utilizzato il seguente comando con il tool hashcat

hashcat -m 0 -a 0 hash.txt /usr/share/wordlists/rockyou.txt

-m indica il tipo di formato di HASH da decifrare il valore 0 indica il formato MD5

-a indica il tipo di attacco, il valore 0 indica un attacco a dizionario con una wordlist

hash.txt è il file che contiene gli HASH da decifrare

rockyou.txt è la wordlist.

Le password decifrate sono queste

5f4dcc3b5aa765d61d8327deb882cf99	password
e99a18c428cb38d5f260853678922e03	abc123
0d107d09f5bbe40cade3de5c71e9e9b7	letmein
8d3533d75ae2c3966d7e0d4fcc69216b	charley