

Formando: Daniel Espada

48bb6e862e54f2a795ffc4e541caed4d (md5) -> easy

```
(espada@kali)-[~]  
$ hashcat -m 0 --show hash1.txt  
48bb6e862e54f2a795ffc4e541caed4d:easy  
(espada@kali)-[~]  
$
```

*Ja tinha feito o comando “hashcat -a 0 -m 0 hash1.txt /usr/share/wordlists/rockyou.txt” e não tirei print, ou seja, tentei fazer de novo para tirar print e dá erro de que todas as hashes já tinham sido encontradas, por isso fiz este comando*

CBFDAC6008F9CAB4083784CBD1874F76618D2A97 (sha\*) -> password123

```
(espada@kali)-[~]  
$ hashcat -a 0 -m 100 hash.txt /usr/share/wordlists/rockyou.txt  
hashcat (v6.2.6) starting  
OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]  
* Device #1: cpu-haswell-Intel(R) Core(TM) i5-8500 CPU @ 3.00GHz, 2898/5861 MB (1024 MB allocatable), 2MCU  
Minimum password length supported by kernel: 0  
Maximum password length supported by kernel: 256  
Hashes: 1 digests; 1 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-Hash  
* 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 hit:  
* Filename..: /usr/share/wordlists/rockyou.txt  
* Passwords.: 14344385  
* Bytes.....: 139921507  
* Keyspace..: 14344385  
cbfdac6008f9cab4083784cbd1874f76618d2a97:password123  
Session.....: hashcat  
Status.....: Cracked  
Hash.Mode.....: 100 (SHA1)  
Hash.Target.....: cbfdac6008f9cab4083784cbd1874f76618d2a97  
Time.Started.....: Fri Jun 6 17:19:23 2025 (0 secs)  
Time.Estimated...: Fri Jun 6 17:19:23 2025 (0 secs)  
Kernel.Feature...: Pure Kernel  
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)  
Guess.Queue.....: 1/1 (100.00%)  
Speed.#1.....: 1823.1 kH/s (0.16ms) @ Accel:512 Loops:1 Thr:1 Vec:8  
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)  
Progress.....: 2048/14344385 (0.01%)  
Rejected.....: 0/2048 (0.00%)  
Restore.Point...: 1024/14344385 (0.01%)  
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1  
Candidate.Engine.: Device Generator  
Candidates.#1...: kucing -> lovers1
```

1C8BFE8F801D79745C4631D09FFF36C82AA37FC4CCE4FC946683D7B336B63032 (sha\*)

-> letmein

```
(espada@kali)-[~]
$ hashcat -a 0 -m 1400 hash.txt /usr/share/wordlists/rockyou.txt

hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: cpu-haswell-Intel(R) Core(TM) i5-8500 CPU @ 3.00GHz, 2898/5861 MB (1024 MB allocatable), 2MCU

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

Hashes: 1 digests; 1 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-Hash
* 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 hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

1c8bfe8f801d79745c4631d09fff36c82aa37fc4cce4fc946683d7b336b63032:letmein

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 1400 (SHA2-256)
Hash.Target.....: 1c8bfe8f801d79745c4631d09fff36c82aa37fc4cce4fc94668 ... b63032
Time.Started.....: Fri Jun  6 17:20:08 2025 (0 secs)
Time.Estimated...: Fri Jun  6 17:20:08 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 1298.1 kH/s (0.30ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 1024/14344385 (0.01%)
Rejected.....: 0/1024 (0.00%)
Restore.Point....: 0/14344385 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate Engine...: Device Generator
```

279412f945939ba78ce0758d3fd83daa (md4) -> Eternity22

```
(ospadan@kali):[~]
$ hashcat -a 0 -m 900 -r /usr/share/hashcat/rules/best64.rule hash4.txt /usr/share/wordlists/rockyou.txt

hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: cpu-haswell-Intel(R) Core(TM) i5-8500 CPU @ 3.00GHz, 2898/5861 MB (1024 MB allocatable), 2MCU

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

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 77

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* 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 hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 1104517645

279412f945939ba78ce0758d3fd83daa:Eternity22

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 900 (MD4)
Hash.Target.....: 279412f945939ba78ce0758d3fd83daa
Time.Started.....: Fri Jun  6 17:30:48 2025 (0 secs)
Time.Estimated...: Fri Jun  6 17:30:48 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Mod.....: Rules (/usr/share/hashcat/rules/best64.rule)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 19508.5 kH/s (3.77ms) @ Accel:512 Loops:77 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 11748352/1104517645 (1.06%)
Rejected.....: 0/11748352 (0.00%)
Restore.Point...: 151552/14344385 (1.06%)
Restore.Sub.#1...: Salt:0 Amplifier:0-77 Iteration:0-77
Candidate.Engine.: Device Generator
```

\$2y\$12\$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX1H68wsRom (consultar página de ajuda do hashcat) -> bleh

```
(espada@kali)-[~]  
$ cat /usr/share/wordlists/rockyou.txt | grep '^....$' | tee rockyou_4char.txt
```

Como soube que a password era so 4 letras, passei todas as palavras que continham 4 letras para um novo ficheiro e corri a partir desse ficheiro. Ps.: o comando foi disponibilizado por um colega.

```
$ hashcat -a 0 -m 3200 hash5.txt rockyou_4char.txt  
hashcat (v6.2.6) starting  
  
OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEF, DISTRO,  
* Device #1: cpu-haswell-Intel(R) Core(TM) i5-8500 CPU @ 3.00GHz, 2898/5861 MB (1024 MB allocat  
  
Minimum password length supported by kernel: 0  
Maximum password length supported by kernel: 72  
  
Hashes: 1 digests; 1 unique digests, 1 unique salts  
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates  
Rules: 1  
  
Optimizers applied:  
* Zero-Byte  
* Single-Hash  
* Single-Salt  
  
Watchdog: Temperature abort trigger set to 90c  
  
Host memory required for this attack: 0 MB  
  
Dictionary cache built:  
* Filename..: rockyou_4char.txt  
* Passwords.: 18152  
* Bytes.....: 91391  
* Keyspace..: 18152  
* Runtime...: 0 secs  
  
Cracking performance lower than expected?  
  
* Append -w 3 to the commandline.  
  This can cause your screen to lag.  
  
* Append -S to the commandline.  
  This has a drastic speed impact but can be better for specific attacks.  
  Typical scenarios are a small wordlist but a large ruleset.  
  
* Update your backend API runtime / driver the right way:  
  https://hashcat.net/faq/wrongdriver  
  
* Create more work items to make use of your parallelization power:  
  https://hashcat.net/faq/morework  
  
$2y$12$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX1H68wsRom:bleh
```