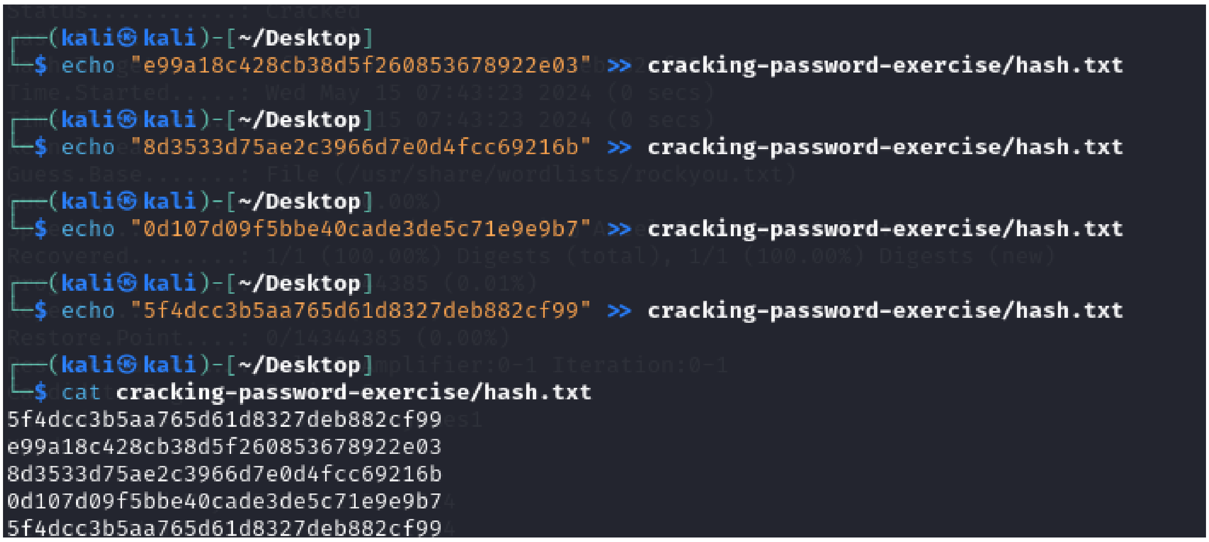
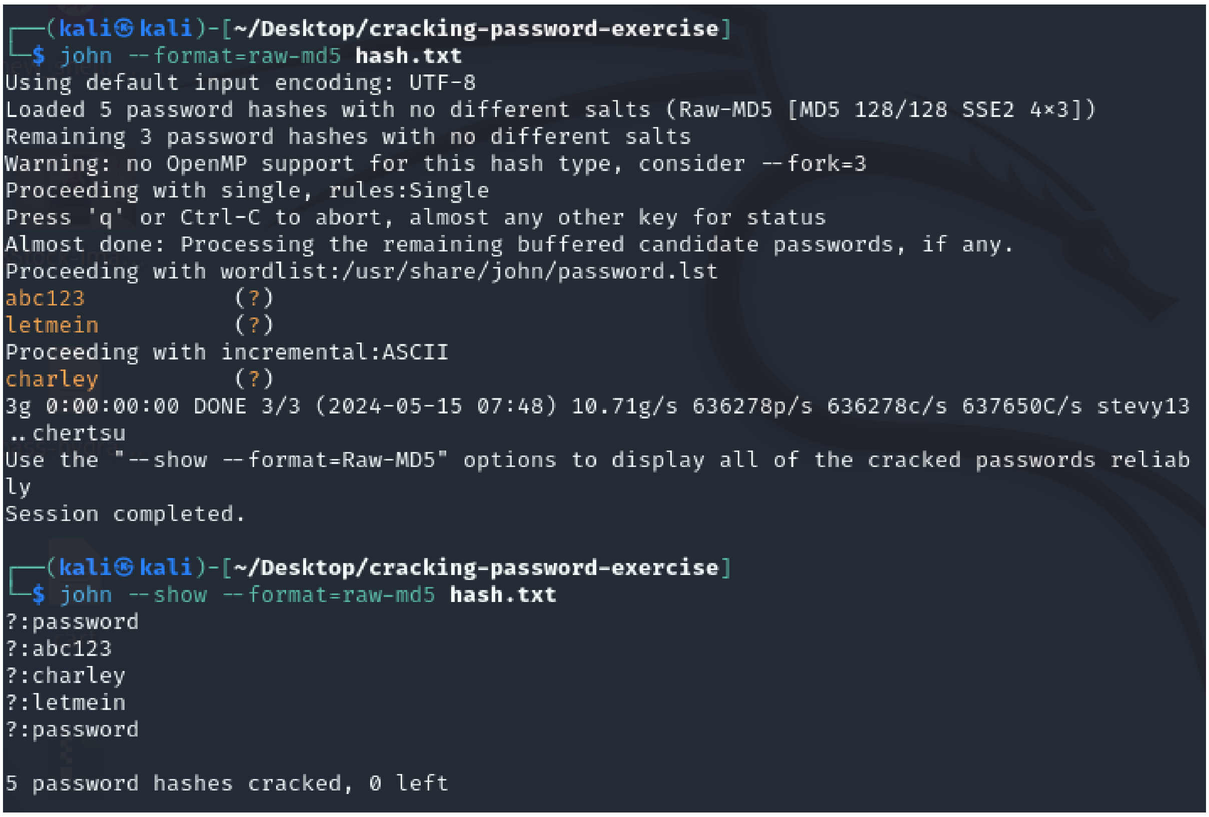
Password cracking (John)

Creazione file txt con i valori MD5 dal terminale



```
┌──(kali㉿kali)-[~/Desktop]
└─$ echo "e99a18c428cb38d5f260853678922e03" >> cracking-password-exercise/hash.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ echo "8d3533d75ae2c3966d7e0d4fcc69216b" >> cracking-password-exercise/hash.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ echo "0d107d09f5bbe40cade3de5c71e9e9b7" >> cracking-password-exercise/hash.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ echo "5f4dcc3b5aa765d61d8327deb882cf99" >> cracking-password-exercise/hash.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ cat cracking-password-exercise/hash.txt
5f4dcc3b5aa765d61d8327deb882cf99
e99a18c428cb38d5f260853678922e03
8d3533d75ae2c3966d7e0d4fcc69216b
0d107d09f5bbe40cade3de5c71e9e9b7
5f4dcc3b5aa765d61d8327deb882cf99
```

Inserire il formato raw-md5 usando John

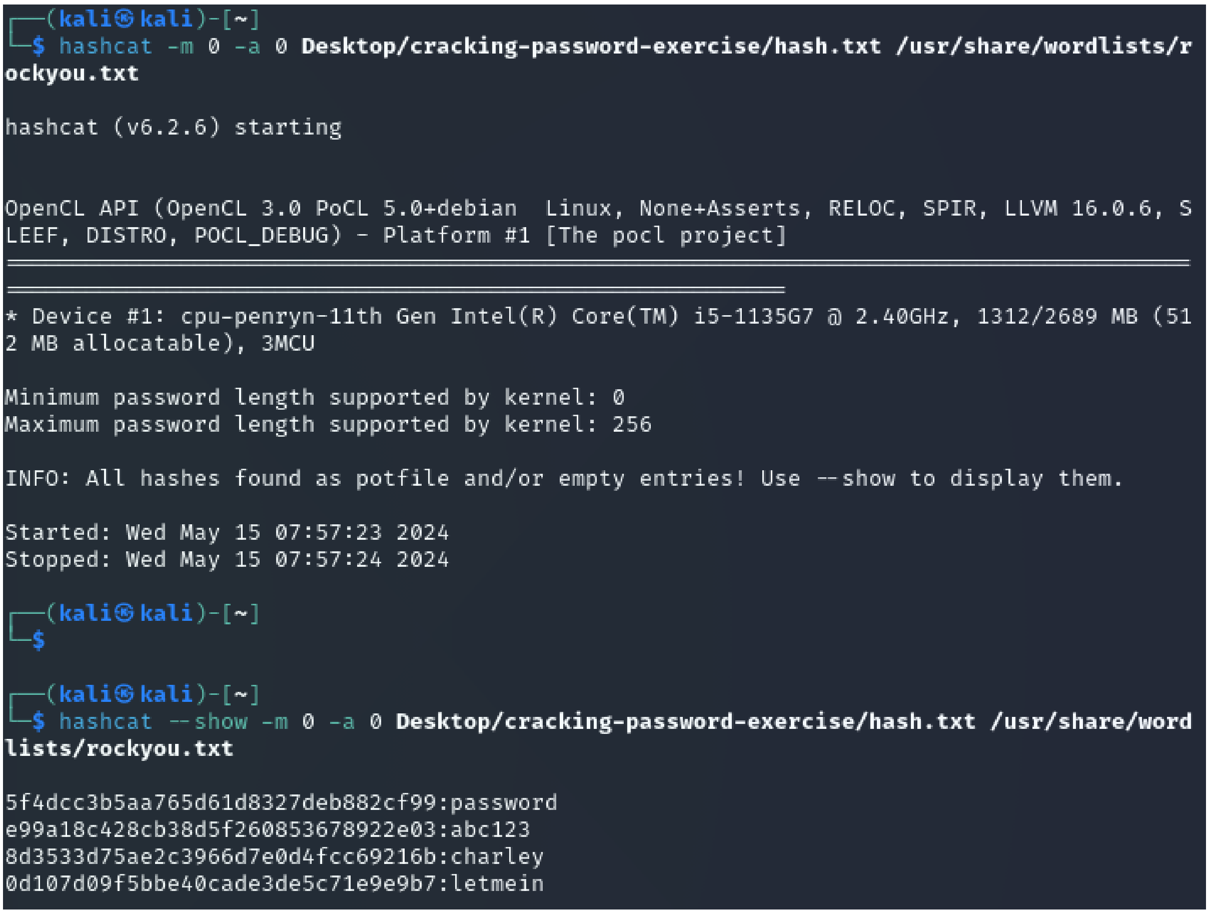


```
┌──(kali㉿kali)-[~/Desktop/cracking-password-exercise]
└─$ john --format=raw-md5 hash.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4×3])
Remaining 3 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=3
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
abc123           (?)
letmein          (?)
Proceeding with incremental:ASCII
charley          (?)
3g 0:00:00:00 DONE 3/3 (2024-05-15 07:48) 10.71g/s 636278p/s 636278c/s 637650C/s stevy13
..chertsu
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliab
ly
Session completed.

┌──(kali㉿kali)-[~/Desktop/cracking-password-exercise]
└─$ john --show --format=raw-md5 hash.txt
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left
```

Utilizzo di –show per vedere la lista delle password che corrispondo a quel MD5

Password cracking (hascat)

Le password sono state trovate prima, questa schermata fa vedere i risultati trovati e il commando che si è utilizzato



```
┌──(kali㉿kali)-[~]
└─$ hashcat -m 0 -a 0 Desktop/cracking-password-exercise/hash.txt /usr/share/wordlists/r
ockyou.txt

hashcat (v6.2.6) starting


OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 16.0.6, S
LEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
════════════════════════════════════════════════════════════════════════════════════════
═══════════════════════════════════════════════════════════
* Device #1: cpu-penryn-11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz, 1312/2689 MB (51
2 MB allocatable), 3MCU

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

INFO: All hashes found as potfile and/or empty entries! Use --show to display them.

Started: Wed May 15 07:57:23 2024
Stopped: Wed May 15 07:57:24 2024

┌──(kali㉿kali)-[~]
└─$

┌──(kali㉿kali)-[~]
└─$ hashcat --show -m 0 -a 0 Desktop/cracking-password-exercise/hash.txt /usr/share/word
lists/rockyou.txt

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

Entrambi tool implementano un dictionary attack verficando il codice MD5 se corrisponde con una password della lista da iterare.