

Nell'esercizio odierno abbiamo una serie di password, che tuttavia non ci vengono restituite in chiaro, ma come hash. Attraverso questa tecnica i siti web possono camuffare le password che hanno nel loro database e renderle incomprensibili ad eventuali Black Hat Hacker.

Esistono, tuttavia dei tool molto potenti (già installati su Kali Linux) che si occupano proprio di decifrare gli hash. Uno di questi è "John the Ripper". Vediamo di seguito come fare per decifrare gli hash dell'esercizio:

- 5f4dcc3b5aa765d61d8327deb882cf99
- e99a18c428cb38d5f260853678922e03
- 8d3533d75ae2c3966d7e0d4fcc69216b
- 0d107d09f5bbe40cade3de5c71e9e9b7
- 5f4dcc3b5aa765d61d8327deb882cf99

Poiché sappiamo già che l'algoritmo di hashing è md5, il comando che utilizziamo su John the Ripper è il seguente: "john --format=raw-md5 --incremental (file da decifrare)". Vediamo il programma in funzione:

```
kali@kali: ~/Desktop
File Actions Edit View Help
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])
No password hashes left to crack (see FAQ)

(kali@kali)-[~/Desktop]
$ john --format=raw-md5 --incremental Hash2.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
abc123 (??)
1g 0:00:00:00 DONE (2024-05-15 11:45) 4.545g/s 59345p/s 59345c/s 59345C/s amb100..abby99
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

(kali@kali)-[~/Desktop]
$ john --format=raw-md5 --incremental Hash3.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
charley (??)
1g 0:00:00:00 DONE (2024-05-15 11:47) 3.571g/s 76114p/s 76114c/s 76114C/s stevy13..chertsu
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

(kali@kali)-[~/Desktop]
$ john --format=raw-md5 --incremental Hash4.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
letmein (??)
1g 0:00:00:00 DONE (2024-05-15 11:48) 1.149g/s 2935Kp/s 2935Kc/s 2935KC/s letebru..letmish
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Otteniamo, così le seguenti password: "charley", "letmein", "abc123", "password".