

CONSEGNA 28 FEBBRAIO S6L3

L'obiettivo di oggi è quello di craccare delle password, mappate in una stringa arbitraria tramite la funzione hash. In Fig.1 vediamo le password criptate che andremo a "tradurre" tramite un tool di Kali, John the Ripper.

```
1 5f4dcc3b5aa765d61d8327deb882cf99
2 e99a18c428cb38d5f260853678922e03
3 8d3533d75ae2c3966d7e0d4fcc69216b
4 0d107d09f5bbe40cade3de5c71e9e9b7
5 5f4dcc3b5aa765d61d8327deb882cf99
```

Fig.1

In Fig.2 possiamo vedere il programma in azione: ho usato la funzione wordlist, che andrà ad attingere password usuali da una lista in rockyou.txt, cripterà la password con la funzione crittografica MD5 e la confronterà con la lista di Fig.1 che ho inserito nel file hash.txt.

```
(kali㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 ./Desktop/hash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8 x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
password      (?)
abc123        (?)
letmein       (?)
charley       (?)
4g 0:00:00:00 DONE (2024-02-28 08:50) 66.66g/s 51200p/s 51200c/s 76800C/s my3
kids..dangerous
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Fig.2

In breve tempo il tool mi ha restituito il risultato (Fig.3), sottolineo che le tempistiche sono state brevi perché le password era semplici, totalmente diverso è se andiamo ad inserire password non convenzionali perché le tempistiche si dilatano : possono volerci giorni.

```
(kali㉿kali)-[~]
└─$ john --show --format=raw-md5 ./Desktop/hash.txt
?:password
?:abc123
?:charley
?:letmein
?:password
5 password hashes cracked, 0 left
```

Fig.3

Ho anche provato ad usare l'incrementale (Fig.4), che funziona diversamente dalla wordlist: tenta di "scovare" la password provando carattere per carattere, ed incrementando lo stesso nella caso di esito negativo della prima prova,. Ho provato ad inserire una password casuale, per vedere se era all'interno di una delle lista offerte da seclists., ma date le tempistiche molto lunghe ho dovuto interrompere il processo.

```
(kali㉿kali)-[~]
$ echo "30secondtoMars" | md5sum
79899b87c76d13e49963c5b848b3e0b7
Try: sudo apt install <deb name>

(kali㉿kali)-[~]
$ john --incremental --format=raw-md5 ./Desktop/hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:21:04 0g/s 26038Kp/s 26038Kc/s 26038KC/s irn2j827..irn2jk1d
0g 0:00:34:51 0g/s 24730Kp/s 24730Kc/s 24730KC/s lytivriidd..lytivrox9
0g 0:00:46:26 0g/s 23875Kp/s 23875Kc/s 23875KC/s sonelandrula..sonelangluie
```

Fig.4