

## ESERCIZIO S6L3

**Traccia:** Password cracking. Sentitevi liberi di utilizzare qualsiasi tool o soluzione alternativa. L'obiettivo dell'esercizio di oggi è craccare tutte le password. Le password da craccare sono le seguenti:

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

## SVOLGIMENTO

Per poter craccare le password in hash scritte sopra si è usato il tool John The Ripper, un password cracking molto noto. Inizialmente si è creato un file che contenesse una lista di tutte le password scritte in hash, il file è stato chiamato **list.txt**.

```
1 5f4dcc3b5aa765d61d8327deb882cf99
2 e99a18c428cb38d5f260853678922e03
3 8d3533d75ae2c3966d7e0d4fcc69216b
4 0d107d09f5bbe40cade3de5c71e9e9b7
5 5f4dcc3b5aa765d61d8327deb882cf99
6
```

Successivamente da terminale Kali, ci si è messi nella shell che contiene il file creato list.txt prima di lanciare John.

```
(kali@kali)-[~/Desktop]
└─$ john --format=raw-md5 --incremental list.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (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
abc123      (?)
charley     (?)
password    (?)
letmein     (?)
4g 0:00:00:00 DONE (2024-05-15 15:12) 4.651g/s 2969Kp/s 2969Kc/s 3486KC/s letero1..letm
ish
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords relia
bly
Session completed.

(kali@kali)-[~/Desktop]
└─$
```

Con il primo comando codifichiamo il "**--format=raw-md5**", specifica il formato dell'hash che si sta cercando di craccare. Nel contesto di un hash MD5, questo indica che il programma dovrebbe interpretare l'hash come un hash MD5.

L'opzione "**--incremental**" in John the Ripper indica che l'attacco condotto sarà un attacco incrementale. Significa che John the Ripper proverà a generare e testare password in modo incrementale, cioè, generando e testando combinazioni di caratteri in modo sequenziale, partendo da una certa lunghezza e procedendo gradualmente fino a raggiungere una lunghezza massima specificata o fino a quando non viene trovata una corrispondenza.

Come si nota dall'immagine in alto, John The Ripper è riuscito a craccare le password scritte in hash e le ha stampate a schermo in colore arancione.

Di seguito scriviamo la password in hash e il corrispettivo in chiaro:

- 5f4dcc3b5aa765d61d8327deb882cf99 → abc123
- e99a18c428cb38d5f260853678922e03 → charley
- 8d3533d75ae2c3966d7e0d4fcc69216b → password
- 0d107d09f5bbe40cade3de5c71e9e9b7 → letmein
- 5f4dcc3b5aa765d61d8327deb882cf99 → abc123