



Manuel Di Gangi

# S6\_L3

## Password cracking

28 febbraio 2024

### Traccia

Se guardiamo meglio le password, della lezione precedente, non hanno l'aspetto di password in chiaro, ma sembrano più hash di password MD5.

Recuperate le password dal DB e provate ad eseguire delle sessioni di cracking sulla password per recuperare la loro versione in chiaro. Sentitevi liberi di utilizzare qualsiasi dei tool visti nella lezione teorica.

**L'obiettivo dell'esercizio di oggi è craccare tutte le password.**





## John the Ripper - Dizionario

1) Effettuiamo un password cracking in loco, lanciando un attacco a dizionario con John the Ripper utilizzando l'opzione `--wordlist`

```
(kali㉿kali)-[~]
$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 ./Desktop/Hash_Crack.txt

Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AV X2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=3
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 08:35) 133.3g/s 102400p/s 102400c/s 153600 C/s my3kids..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.
```

2) Stampiamo a video il risultato delle operazioni

```
(kali㉿kali)-[~]
$ john --show --format=raw-md5 ./Desktop/Hash_Crack.txt

?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left
```

## John the Ripper - Incrementale

Qualora l'operazione precedente dovesse non trovare alcune password, nel caso di password complicate, possiamo provare con la modalità incrementale. Con questo metodo John testa tutte le possibili combinazioni di caratteri finché non trova la password corrispondente.

```
(kali㉿kali)-[~]
$ john --incremental --format=raw-md5 ./Desktop/Hash_Crack.txt
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AV
X2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=3
Press 'q' or Ctrl-C to abort, almost any other key for status
abc123          (?)
charley         (?)
password        (?)
letmein         (?)
4g 0:00:00:01 DONE (2024-02-28 08:59) 2.666g/s 1702Kp/s 1702Kc/s 1998KC/s
letero1..letmish
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked p
asswords reliably
Session completed.

(kali㉿kali)-[~]
$ john --show --format=raw-md5 ./Desktop/Hash_Crack.txt
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left
```