Esercizio S6-L3

```
C:\home\kali\.john> john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-MD5 /home/kali/Desktop/hash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8×3])
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 16:27) 200.0g/s 153600p/s 153600c/s 230400C/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.

C:\home\kali\.john> sudo rm *

C:\home\kali\.john> john --incremental --format=raw-MD5 /home/kali/Desktop/hash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8×3])
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 0:00:00:02 DONE (2024-02-28 16:27) 1.913g/s 1222Kp/s 1222Kc/s 1434KC/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 passwords reliably
Session completed.
```

Una volta effettuato l'SQL Injection [Esercizio S6-L3] e recuperate le varie password in formato hash, abbiamo utilizzato JohnTheRiper per poter confrontare gli hash ricavati, da hash di password in chiaro contenute in un file di testo. Abbiamo quindi effettuato un attacco a forza bruta, prima grazie al metodo wordlist e poi grazie al metodo incrementale. I risultati di entrambi gli attacchi corrispondevano alle password contenute nel database.