



Traccia: password cracking

Abbiamo visto come sfruttare un attacco SQL injection per recuperare le password degli utenti di un determinato sistema.

Se guardiamo meglio alle password trovate, non hanno l'aspetto di password in chiaro, ma sembrano più hash di password MD5.

Recuperate le password dal DB come visto, 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 trovate precedentemente.

Consegna:

1. Screenshot dell'SQL injection già effettuata
2. Due righe di spiegazione di cos'è questo cracking (quale tipologia / quale meccanismo sfrutta)
3. Screenshot dell'esecuzione del cracking e del risultato

```
Home kali@kali: ~
(kali@kali)-[~]
$ john --format=raw-md5 --wordlist /usr/share/wordlists/rockyou.txt ./Desktop/Hash.txt
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 55 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Remaining 54 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=8
Proceeding with wordlist:/usr/share/john/password.lst
Press 'q' or Ctrl-C to abort, almost any other key for status
password      (?)
abc123         (?)
letmein        (?)
3g 0:00:00:00 DONE (2024-02-07 16:21) 150.0g/s 177300p/s 177300c/s 9099KC/s !@#$%..sss
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.

(kali@kali)-[~]
$ john --show --format=raw-md5 ./Desktop/Hash.txt
?:password
?:abc123
?:letmein
?:password

4 password hashes cracked, 1 left
```

Utilizzando il tool John the Ripper con il flag `-wordlist` abbiamo dato in pasto allo stesso un file che contiene una wordlist con una serie di password ed i rispettivi hash insieme al file degli hash catturati.

Come si vede dallo screenshot il tool ha fatto dei confronti e trovato dei match positivi tra gli hash, grazie ai quali riusciamo a risalire alle password.