

Report: Password Cracking con John the Ripper

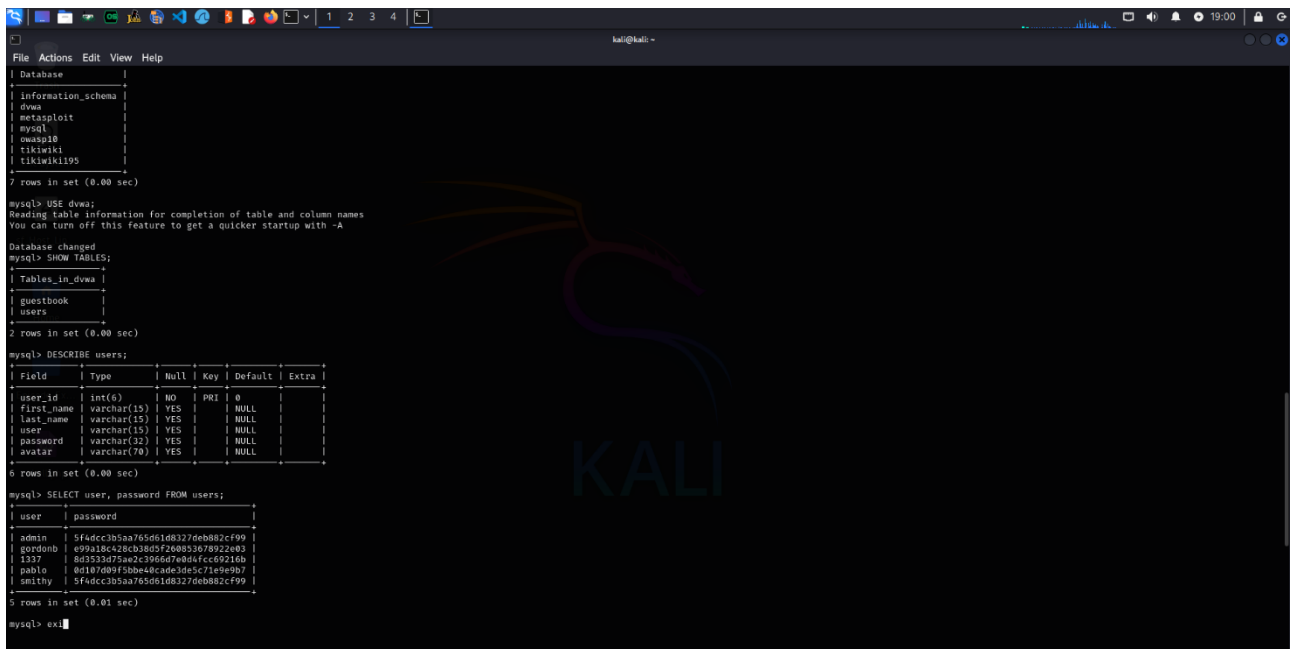
1. Introduzione

In questo esercizio ho simulato un attacco per il recupero delle password degli utenti di Metasploitable. Dopo aver eseguito una **SQL Injection** per estrarre le credenziali, ho trovato delle password in formato hash MD5.

2. SQL Injection e Recupero degli Hash

Ho effettuato un attacco **SQL Injection** per accedere al database del sistema e recuperare le credenziali degli utenti. Dopo aver eseguito la query malevola, abbiamo ottenuto un elenco di hash di password in formato **MD5**.

Screenshot della SQL Injection:



```
mysql> USE dvwa;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> SHOW TABLES;
+-----+
| Tables_in_dvwa |
+-----+
| guestbook      |
| users          |
+-----+
2 rows in set (0.00 sec)

mysql> DESCRIBE users;
+----+-----+-----+-----+-----+-----+
| Field | Type | Null | Key | Default | Extra |
+----+-----+-----+-----+-----+-----+
| user_id | int(6) | NO | PRI | 0 | |
| first_name | varchar(15) | YES | | NULL | |
| last_name | varchar(15) | YES | | NULL | |
| user | varchar(15) | YES | | NULL | |
| password | varchar(32) | YES | | NULL | |
| avatar | varchar(70) | YES | | NULL | |
+----+-----+-----+-----+-----+-----+
6 rows in set (0.00 sec)

mysql> SELECT user, password FROM users;
+-----+-----+
| user | password |
+-----+-----+
| admin | 5f4dcc3b5aa765d61d8327deb882cf99 |
| gordonb | e99118c428c8b8d5f208853678922e03 |
| 1517 | 6d333075a02c3956d7e0a4fccc02168 |
| pablo | 0d187d99f3bbe44cade3de5c71e9e9b7 |
| smithy | 5f4dcc3b5aa765d61d8327deb882cf99 |
+-----+-----+
5 rows in set (0.01 sec)

mysql> exit
```

3. Cracking degli Hash con John the Ripper

Per decriptare gli hash, ho usato il tool **John the Ripper** con il seguente metodo:

Passaggi seguenti:

1. Verifica del file contenente gli hash

Ho controllato che il file hash.txt contenesse correttamente gli hash estratti.

2. Identificazione del tipo di hash

Poiché gli hash sembravano essere **MD5**, ho confermato il formato e proceduto con il cracking.

3. Cracking con John the Ripper

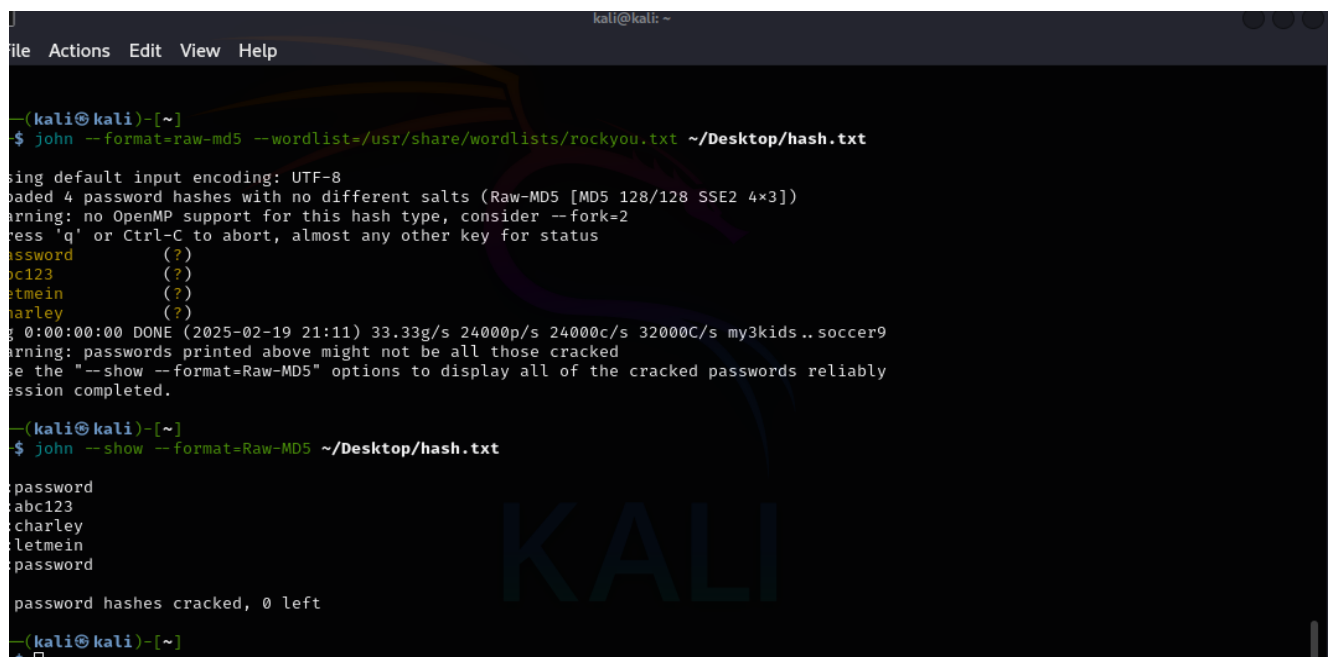
Ho usato una wordlist predefinita (rockyou.txt) per tentare il recupero delle password:

4. Visualizzazione delle password trovate

Dopo il cracking, ho verificato le password recuperate.

4. Risultati

John the Ripper ha trovato con successo le seguenti password associate agli hash:



```
kali@kali: ~  
file Actions Edit View Help  
--(kali@kali)-[~]  
$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt ~/Desktop/hash.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=2  
Press 'q' or Ctrl-C to abort, almost any other key for status  
password (??)  
abc123 (??)  
letmein (??)  
charley (??)  
g 0:00:00:00 DONE (2025-02-19 21:11) 33.33g/s 24000p/s 24000c/s 32000C/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.  
--(kali@kali)-[~]  
$ john --show --format=Raw-MD5 ~/Desktop/hash.txt  
password  
abc123  
charley  
letmein  
password  
password hashes cracked, 0 left  
--(kali@kali)-[~]  
$
```