Il primo passaggio è stato quello di reperire gli hash delle password degli utenti nel database di dvwa e per fare ció ho eseguito i comandi su metasploitable:

```
msfadmin@metasploitable:/var/www/dvwa$ mysql -u root
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 21210
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

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> SELECT user, password FROM users;
+---------+----------------------------------+
| user    | password                         |
+---------+----------------------------------+
| admin   | 5f4dcc3b5aa765d61d8327deb882cf99 |
| gordonb | e99a18c428cb38d5f260853678922e03 |
| 1337    | 8d3533d75ae2c3966d7e0d4fcc69216b |
| pablo   | 0d107d09f5bbe40cade3de5c71e9e9b7 |
| smithy  | 5f4dcc3b5aa765d61d8327deb882cf99 |
+---------+----------------------------------+
5 rows in set (0.00 sec)
```

Dopo aver ottenuto l'hash table, sono andato a verificare come richiesto se fosse di tipo MD5, cosí cercando online ho trovato il tool preinstallato su kali "hash-identifier" che mi ha confermato si trattasse di un hash di tipo MD5

Dopo aver ottenuto le informazioni necessarie per eseguire l'attacco, sono andato a usare john per l'attacco brute force dictionary usando rockyou.txt come dizionario per l'attacco.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john hashes.txt --wordlist=/usr/share/wordlists/rockyou.txt --format=Raw-MD5
Using default input encoding: UTF-8
```

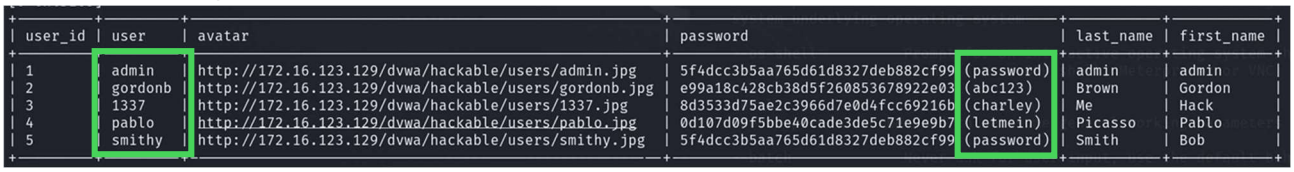
Usando il comando precedente ho effettuato un attacco usando il dizionario (wordlist) rockyou, il formato di dehashing per MD5 e ho dato in input il file contenente tutte le sequenza hash.
A fine scansione, usando il comando:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --show --format=Raw-MD5 hashes.txt
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left
```

Sono andato a visualizzare tutte le password in chiaro e ho notato che la prima e l'ultima password sono uguali e quindi usano la stessa password.

Per la conferma ho effettuato il dump della tabella users nel database dvwa fatto due esercizi fa e conferma che le password sono corrette:



user_id	user	avatar	password	last_name	first_name
1	admin	http://172.16.123.129/dvwa/hackable/users/admin.jpg	5f4dcc3b5aa765d61d8327deb882cf99 (password)	admin	admin
2	gordonb	http://172.16.123.129/dvwa/hackable/users/gordonb.jpg	e99a18c428cb38d5f260853678922e03 (abc123)	Brown	Gordon
3	1337	http://172.16.123.129/dvwa/hackable/users/1337.jpg	8d3533d75ae2c3966d7e0d4fcc69216b (charley)	Me	Hack
4	pablo	http://172.16.123.129/dvwa/hackable/users/pablo.jpg	0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)	Picasso	Pablo
5	smithy	http://172.16.123.129/dvwa/hackable/users/smithy.jpg	5f4dcc3b5aa765d61d8327deb882cf99 (password)	Smith	Bob