Attacco alle password

Oggi andiamo a fare un attacco alle password a dizionario con lo strumento John the ripper. Questo tool fa uso della parallelizzazione dei task per ridurre il tempo di cracking.

Qui sotto riportato l'sql map dell'esercizio di ieri da qui ho preso le password criptate.

```
| 1       | admin   | http://172.16.123.129/dvwa/hackable/users/admin.jpg   | 5f4dcc3b5aa765d61d8327deb882cf99 | ad
min     | admin   |
| 2       | gordonb | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 | Br
own     | 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 | Pi
casso   | Pablo   |
| 5       | smithy  | http://172.16.123.129/dvwa/hackable/users/smithy.jpg  | 5f4dcc3b5aa765d61d8327deb882cf99 | Sm
ith     | Bob     |
```

Ho poi messo gli utenti con le rispettive password in sequenza, in un file chiamato passwd_ash.txt.

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

Per permettere poi il funzionamento di JOHN ho dovuto unzippare il file rockyou che è una lista di password note e molto usate.

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

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

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

Una volta fatte tutti questi passaggi passiamo al vero utilizzo. Utilizziamo il comando riportato qui sotto dove: **--fort=raw-md5** sta ad indicare il formato del criptaggio delle password; nel nostro caso andremo a fare un attacco a dizionario con il comando **–wordlist** seguito dal percorso del "dizionario"; infine il percorso del file con gli utenti e le password.

```
┌──(kali㉿kali)-[~]
└─$ sudo john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt /home/kali/Desktop/passwd_ash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=3
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 09:55) 57.14g/s 41142p/s 41142c/s 54857C/s my3kids..soccer9
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.
```

Poi se si vuole vedere il risultato del nostro operato si può usare il comando riportato qui sotto.

```
┌──(kali㉿kali)-[~]
└─$ sudo john --show --format=raw-md5 /home/kali/Desktop/passwd_ash.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left
```