

ESERCITAZIONE S6 L3

Per recuperare le password in chiaro è stato utilizzato il tool John the Ripper. Per prima cosa abbiamo creato un file contenente user e pass di ieri, chiamato hash.txt.

```
GNU nano 7.2
admin:5f4dcc3b5aa765d61d8327deb882cf99
gordonb:e99a18c428cb38d5f260853678922e03
1337:8d3533d75ae2c3966d7e0d4fcc69216b
pablo:0d107d09f5bbe40cade3de5c71e9e9b7
smithy:5f4dcc3b5aa765d61d8327deb882cf99
```

Poi abbiamo estratto il file rockyou.txt presente nel percorso:
/usr/share/wordlists/

Aprendo il terminale e inserendo il seguente comando possiamo crackare le password degli user scoperti ieri.

john --format=raw-md5 --wordlist=/home/kali/Desktop/rockyou.txt hash.txt

```
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ john --format=raw-md5 --wordlist=/home/kali/Desktop/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])
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 (2024-01-10 16:34) 133.3g/s 96000p/s 96000c/s 128000C/s my3kids..soc
cer9
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliab
ly
Session completed.
```

Possiamo notare come non tutte le password sono state crackate, utilizzando il comando *john --format=raw-md5 --show /home/kali/Desktop/rockyou.txt hash.txt* possiamo scoprire tutte le password in chiaro.

```
(kali@kali)-[~/Desktop]
$ john --format=raw-md5 --show /home/kali/Desktop/rockyou.txt hash.txt
Warning: invalid UTF-8 seen reading /home/kali/Desktop/rockyou.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 52 left
```