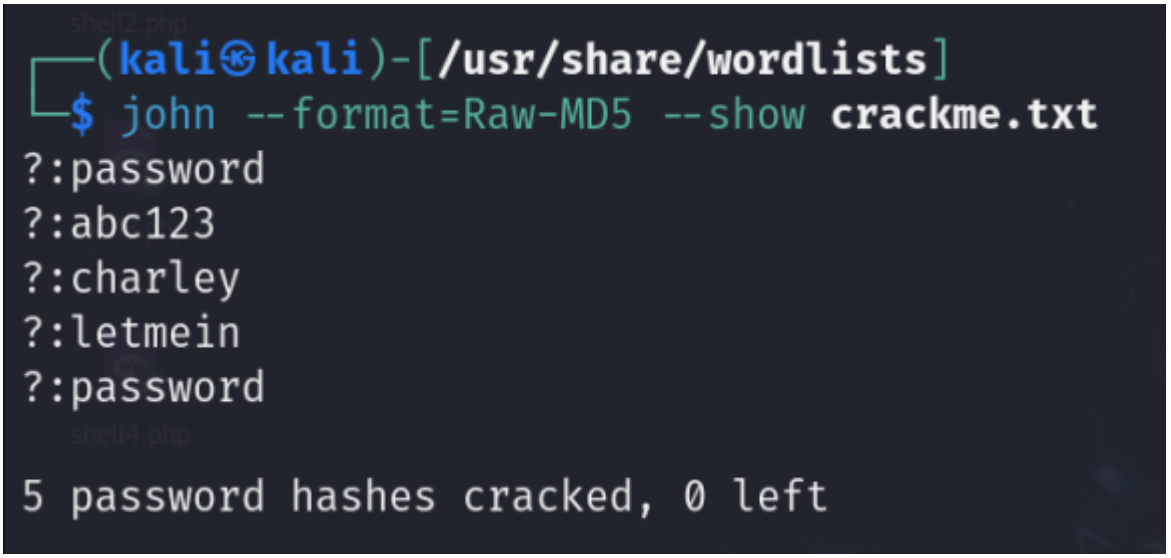
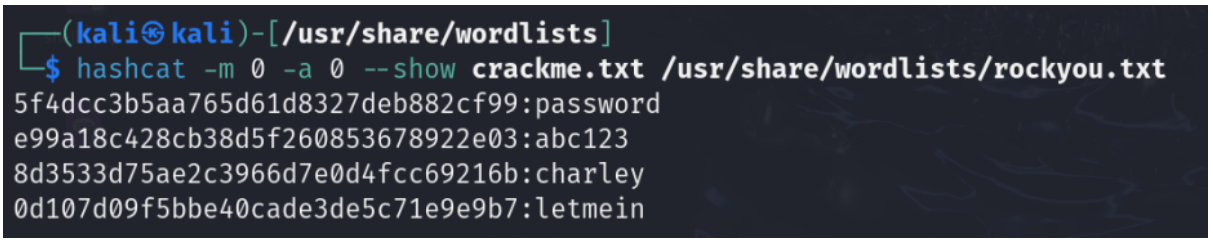
Utilizziamo vari tools per il cracking delle password date dalla traccia.

Con John The Ripper (comunemente **john**):
Selezioniamo il formato dell'hash e mostriamo le password crackate all'interno del file che abbiamo chiamato crackme.txt



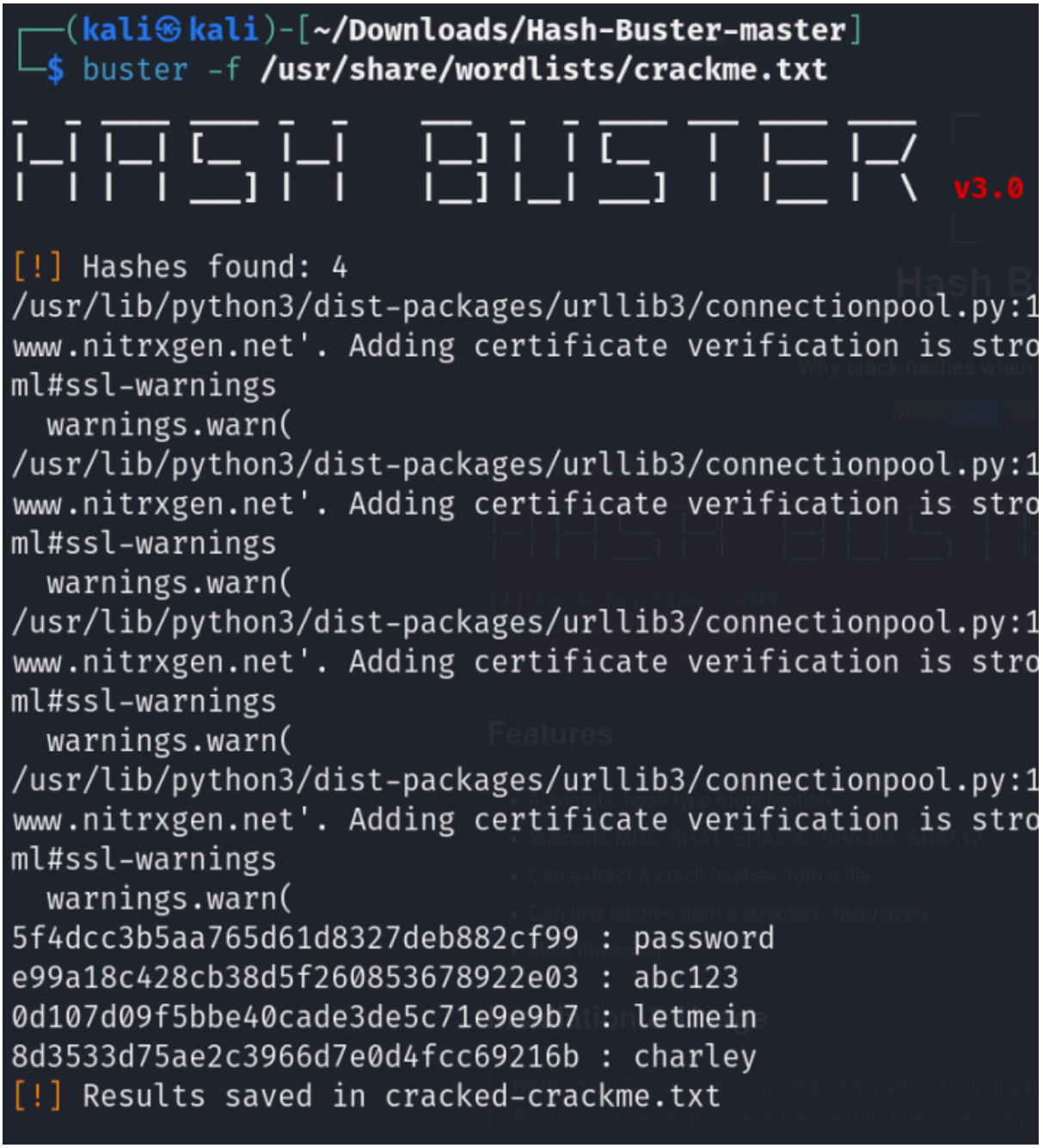
Proviamo con **hashcat:**



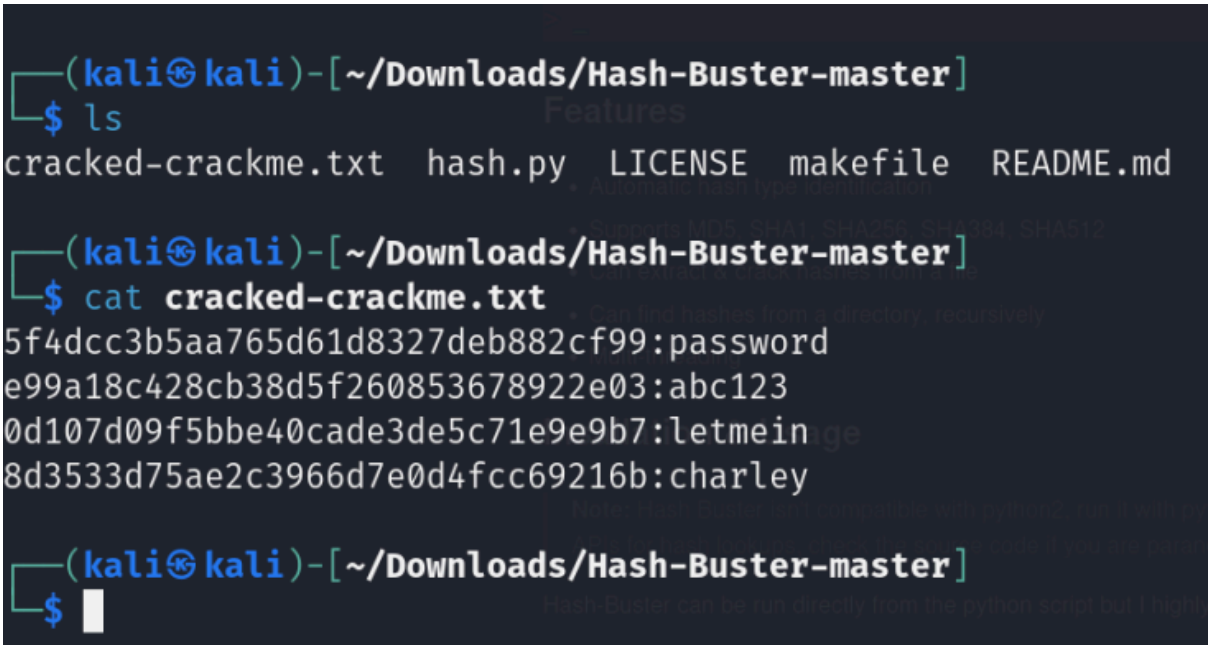
dove -m 0 sta ad indicare il formato dell'hash(MD5), -a 0 indica un tipo di attacco a dizionario, –show mostra le password decriptate dalla wordlist **rockyou.txt**
Essendo presenti due hash uguali dati dalla traccia, ovviamente rockyou.txt mostrerà il risultato solo del primo hash (quindi *password*).

Un altro tool carino ed efficace che ho utilizzato fa riferimento ad Hash Buster.

Qui, come possiamo notare, non abbiamo bisogno di specificare il formato dell'hash, dato che Hash Buster lo identificherà in automatico e procederà con il cracking delle password, mostrandoci quanto segue:



Inoltre, come si evince dalla figura, automaticamente salverà un file di testo chiamato cracked-crackme.txt dove all'interno verranno salvate tutte le password trovate.


┌──(kali㉿kali)-[~/Downloads/Hash-Buster-master]
└─$ ls
cracked-crackme.txt hash.py LICENSE makefile README.md
┌──(kali㉿kali)-[~/Downloads/Hash-Buster-master]
└─$ cat cracked-crackme.txt
5f4dcc3b5aa765d61d8327deb882cf99:password
e99a18c428cb38d5f260853678922e03:abc123
0d107d09f5bbe40cade3de5c71e9e9b7:letmein
8d3533d75ae2c3966d7e0d4fcc69216b:charley
┌──(kali㉿kali)-[~/Downloads/Hash-Buster-master]
└─$