

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

```
shell2.php
(kali㉿kali)-[/usr/share/wordlists]
$ john --format=Raw-MD5 --show crackme.txt
?:password
?:abc123
?:charley
?:letmein
?:password
shell4.php
5 password hashes cracked, 0 left
```

Proviamo con **hashcat**:

```

(kali㉿kali)-[/usr/share/wordlists]
$ hashcat -m 0 -a 0 --show crackme.txt /usr/share/wordlists/rockyou.txt
5f4dcc3b5aa765d61d8327deb882cf99:password
e99a18c428cb38d5f260853678922e03:abc123
8d3533d75ae2c3966d7e0d4fcc69216b:charley
0d107d09f5bbe40cade3de5c71e9e9b7:letmein
```

dove -m 0 sta ad indicare il formato dell'hash(MD5), -a 0 indica un tipo di attacco a dizionario, --show mostra le password deciptate 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.

```

(kali㉿kali)-[~/Downloads/Hash-Buster-master]
$ buster

HASH BUSTER v3.0
```

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:

```
(kali㉿kali)-[~/Downloads/Hash-Buster-master]
$ buster -f /usr/share/wordlists/crackme.txt

HASH BUSTER v3.0

[!] Hashes found: 4
/usr/lib/python3/dist-packages/urllib3/connectionpool.py:1
www.nitrxgen.net'. Adding certificate verification is stro
ml#ssl-warnings
  warnings.warn(
/usr/lib/python3/dist-packages/urllib3/connectionpool.py:1
www.nitrxgen.net'. Adding certificate verification is stro
ml#ssl-warnings
  warnings.warn(
/usr/lib/python3/dist-packages/urllib3/connectionpool.py:1
www.nitrxgen.net'. Adding certificate verification is stro
ml#ssl-warnings
  warnings.warn(
/usr/lib/python3/dist-packages/urllib3/connectionpool.py:1
www.nitrxgen.net'. Adding certificate verification is stro
ml#ssl-warnings
  warnings.warn(
5f4dcc3b5aa765d61d8327deb882cf99 : password
e99a18c428cb38d5f260853678922e03 : abc123
0d107d09f5bbe40cade3de5c71e9e9b7 : letmein
8d3533d75ae2c3966d7e0d4fcc69216b : charley
[!] Results saved in cracked-crackme.txt
```

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]
```

```
$
```