

S6-L3

Password Cracking.

L'obiettivo dell'esercizio di oggi è craccare tutte le password.

Le password da craccare sono le seguenti:

- 5f4dcc3b5aa765d61d8327deb882cf99
- e99a18c428cb38d5f260853678922e03
- 8d3533d75ae2c3966d7e0d4fcc69216b
- 0d107d09f5bbe40cade3de5c71e9e9b7
- 5f4dcc3b5aa765d61d8327deb882cf99

Il Tool

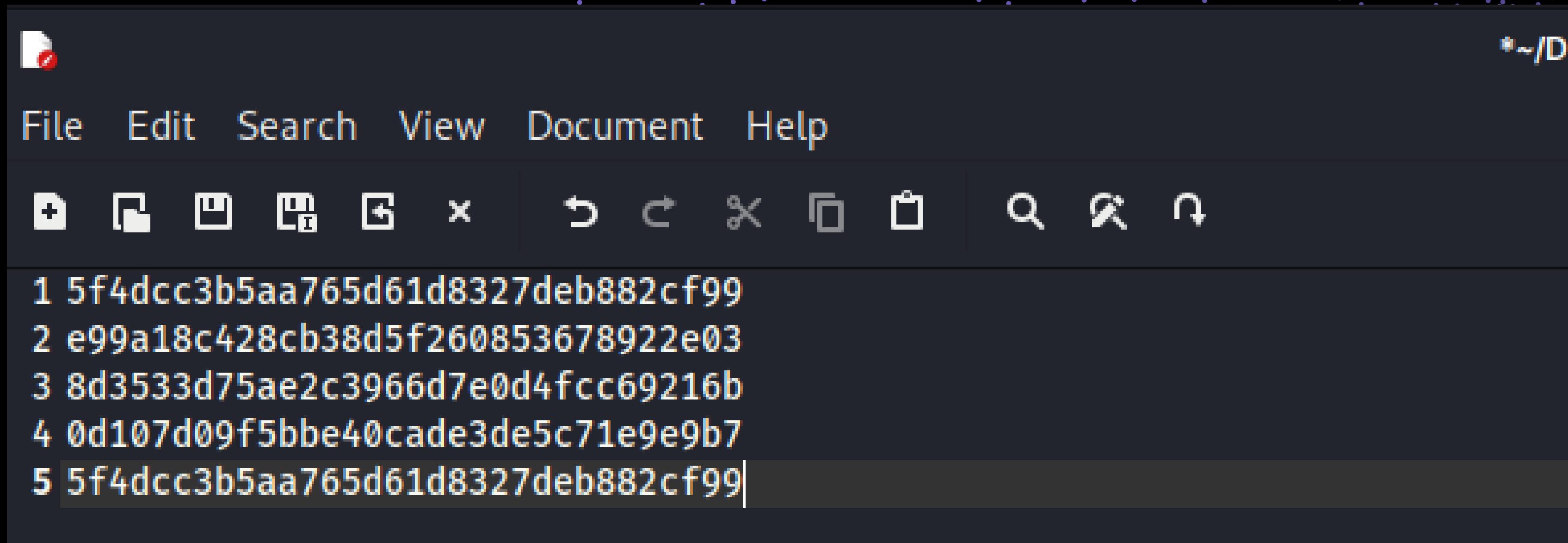
Utilizzato è John the Ripper

John the Ripper è uno strumento di cracking delle password, supporta numerosi algoritmi di hashing, tra cui MD5, SHA-1, SHA-256, bcrypt, decrypt, LM hash (utilizzato in Windows), e molti altri.

Abbiamo a disposizione diversi tipi di attacchi ad esempio:

- Attacco a Dizionario: Utilizza una lista di parole (wordlist) per tentare di crackare le password confrontandole con gli hash.
- Attacco Incrementale: Prova tutte le combinazioni possibili di caratteri fino a trovare una corrispondenza, iniziando dalle combinazioni più semplici.
- Attacco a Regole: Applica regole di manipolazione delle parole su una wordlist per generare varianti complesse delle password

La tipologia di attacco che andremo ad utilizzare
è un attacco incrementale sull'algoritmo di
hashing MD5



A screenshot of a terminal window with a dark background. The window title bar shows a file icon and the path '~/.D'. The menu bar includes 'File', 'Edit', 'Search', 'View', 'Document', and 'Help'. Below the menu is a toolbar with various icons. The main area contains a list of five MD5 hash values:

```
1 5f4dcc3b5aa765d61d8327deb882cf99
2 e99a18c428cb38d5f260853678922e03
3 8d3533d75ae2c3966d7e0d4fcc69216b
4 0d107d09f5bbe40cade3de5c71e9e9b7
5 5f4dcc3b5aa765d61d8327deb882cf99|
```

Andiamo a creare un file di testo contenente le password da craccare

L'opzione “**--format=raw-md5**“ si specifica il formato dell'hash che si sta cercando di craccare, in questo caso md5 e l'opzione “**--incremental**“ indica che l'attacco condotto sarà un attacco incrementale.

```
(kali㉿kali)-[~/Desktop]
$ john --format=raw-md5 --incremental hash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
abc123      (?)
charley      (?)
password     (?)
letmein      (?)
4g 0:00:00:02 DONE (2024-05-15 15:19) 1.465g/s 935525p/s 935525c/s 1098KC/s letero1.. le
tmish
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.
```

Questo è l'output del comando completo **john --format=raw-md5 --incremental nomefile.txt** e come possiamo notare, il nostro attacco è andato a buon fine

Dall'immagine precedente, possiamo vedere che il programma ci fornisce un consiglio su come visualizzare le password craccate, utilizzando il comando **john --show --format=Raw-MD5 nomefile.txt**

```
(kali㉿kali)-[~/Desktop]
$ john --show --format=Raw-MD5 hash.txt
?:password
?:abc123
?:charley
?:letmein
?:password
```

Nel caso in cui si siano stati dei problemi, possiamo utilizzare il comando **rm ~/.john/john.pot** per rimuovere il file e poter effettuare nuovamente l'attacco e visualizzare le nuove password craccate

```
(kali㉿kali)-[~/Desktop]
$ rm ~/.john/john.pot
```