

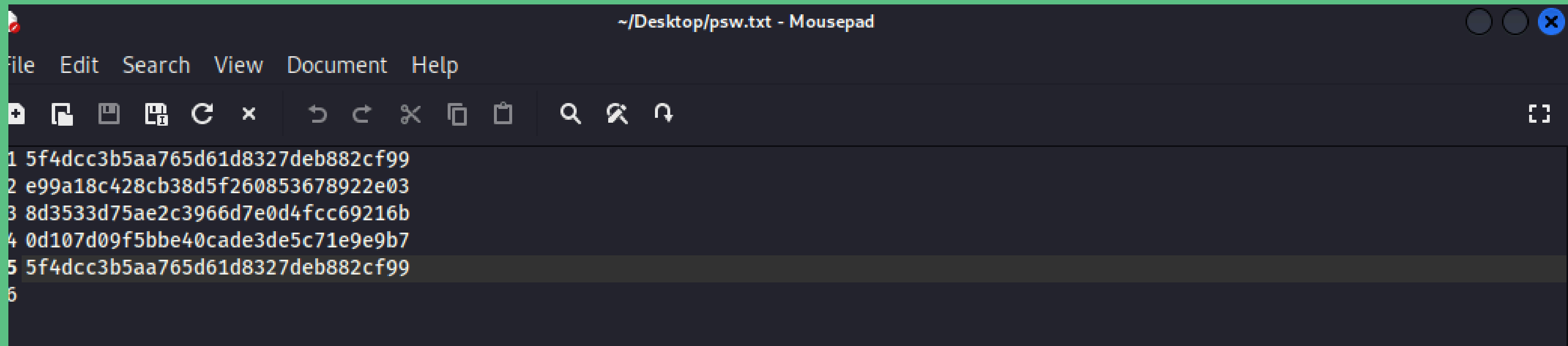


PASSWORD CRACKING

MORGAN PETRELLI S6/L3

**L'OBIETTIVO DELL'ESERCIZIO DI OGGI È CRACCARE TUTTE LE
PASSWORD. LE PASSWORD DA CRACCARE SONO LE SEGUENTI:**

- **5F4DCC3B5AA765D61D8327DEB882CF99**
- **E99A18C428CB38D5F260853678922E03**
- **8D3533D75AE2C3966D7E0D4FCC69216B**
- **0D107D09F5BBE40CADE3DE5C71E9E9B7**
- **5F4DCC3B5AA765D61D8327DEB882CF99**



The screenshot shows a window titled "~/Desktop/psw.txt - Mousepad". The menu bar includes File, Edit, Search, View, Document, and Help. The toolbar contains icons for opening, saving, undo, redo, cut, copy, paste, search, and zoom. The text area contains the following content:

```
1 5f4dcc3b5aa765d61d8327deb882cf99
2 e99a18c428cb38d5f260853678922e03
3 8d3533d75ae2c3966d7e0d4fcc69216b
4 0d107d09f5bbe40cade3de5c71e9e9b7
5 5f4dcc3b5aa765d61d8327deb882cf99
6
```

**HO INIZIALMENTE
CREATO UN FILE .TXT
CONTENENTE LE
PASSWORD IN ASCII**

con il comando

john --format=raw-md5 --incremental

psw.txt

ho avviato John the Ripper inizierà a eseguire un attacco di forza bruta per cercare tutte le possibili combinazioni di caratteri fino a trovare le password corrispondenti agli hash forniti nel file psw.txt.

“--format=raw-md5” specifica il formato dell'hash delle password

“--incremental” indica a John the Ripper di eseguire un attacco di forza bruta.

```
(kali㉿kali)-[~/Desktop]
└─$ john --format=raw-md5 --incremental psw.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, con
sider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key
for status
abc123          (?)
charley         (?)
password        (?)
letmein         (?)
4g 0:00:00:01 DONE (2024-05-15 15:56) 2.898g/s 185
0Kp/s 1850Kc/s 2172KC/s letebru..letmish
Warning: passwords printed above might not be all
those cracked
Use the "--show --format=Raw-MD5" options to displ
ay all of the cracked passwords reliably
Session completed.
```

PER USARE JOHN THE RIPPER PER FARE
UN DICTIONARY ATTACK HO USATO IL
COMANDO

```
JOHN --FORMAT=RAW-MD5 --  
WORDLIST=/USR/SHARE/WORDLIST/ROCKYOU.TXT PSW.TXT
```

JOHN THE RIPPER INIZIERÀ A TESTARE
OGNI PAROLA CHE SI TROVANO NEL FILE
DI TESTO ROCKYOU CONTRO GLI HASH
NEL FILE PWD.TXT.

```
$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt psw.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

password	(?)
abc123	(?)
letmein	(?)
charley	(?)

4g 0:00:00:00 DONE (2024-05-15 13:06) 200.0g/s 153600p/s 153600c/s 230400C/s my3kids..dangerous
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.