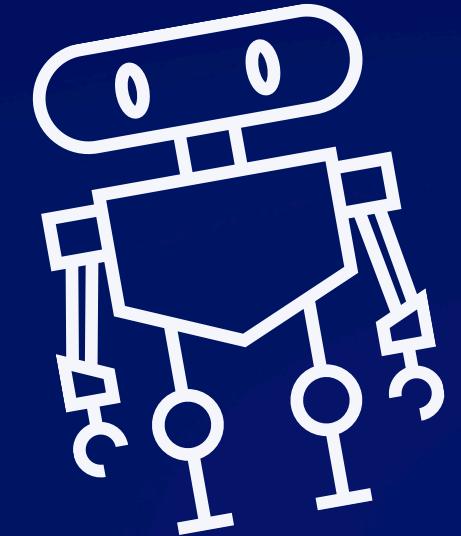
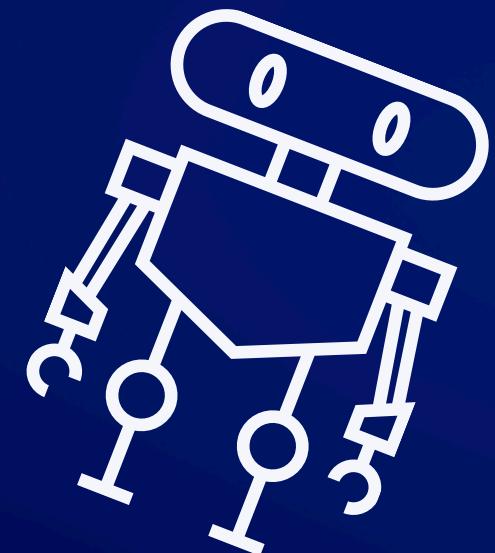




Password Cracking

56/L3



Mara Dello Russo

Introduzione

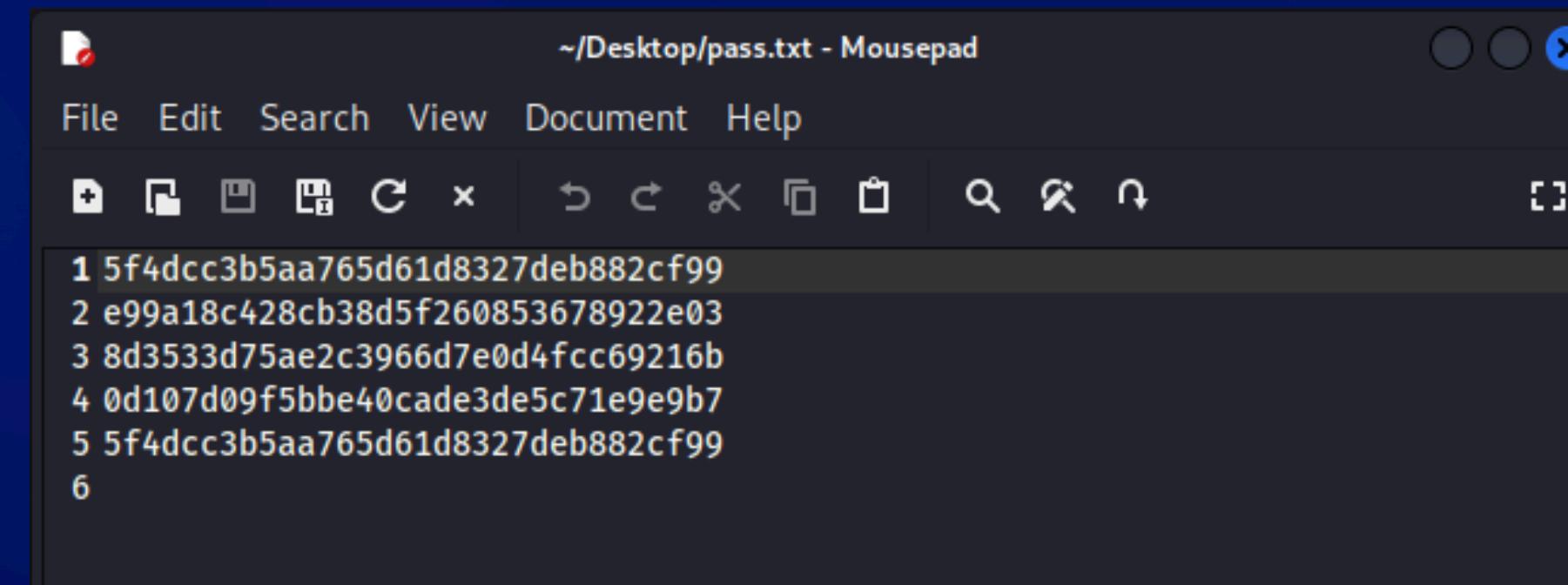
Password cracking è il processo di recupero di password o di altre credenziali di autenticazione da dati memorizzati o trasmessi da un sistema informatico. Questo processo può utilizzare una varietà di tecniche, che vanno dagli attacchi a forza bruta agli attacchi a dizionario, fino agli attacchi basati su rainbow table, phishing e altri tipi di exploit.

Esistono diversi strumenti usati per il password cracking. Nel nostro esempio andremo ad utilizzare **John The Ripper**

Craccare le seguenti password:

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

Creiamo un file di testo (in questo caso pass.txt) in cui inseriamo le password che dobbiamo craccare.



Da linea di comando eseguiamo

john --format=raw-md5 --incremental pass.txt

```
(kali㉿kali)-[~/Desktop]
$ john --format=raw-md5 --incremental pass.txt
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8×3])
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 15:41) 1.486g/s 949436p/s 949436c/s 1114KC/s letero1..letmish
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.
```

- **john**: comando per avviare John the Ripper
- **--format=raw-md5**: specifica che il formato dell'hah è MD5
- **--incremental**: indica che John deve usare l'attacco incrementale, cioè il brute force
- **pass.txt**: file che contiene gli hash MD5 da craccare

In questo caso possiamo subito intuire che l'algoritmo utilizzato per trasformare la password in hash è l'MD5 perché presenta 32 caratteri esadecimali.

Nel caso non fossimo in grado di capire l'algoritmo utilizzato con la sola visione degli hash potremmo utilizzare tool come **hashid** che analizzeranno l'hash che gli forniamo in riga di comando e identificheranno l'algoritmo utilizzato.

John the Ripper in output ci mostra soltanto 4 password in chiaro delle 5 che gli abbiamo fornito in input, perché una di esse è un duplicato.

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

5 password hashes cracked, 0 left
```

Con il comando
john --show --format=raw-MD5 pass.txt
possiamo vedere in ordine le password craccate.

GRAZIE PER
L'ATTENZIONE

