

Noemi  
de Martino

S6//L3

PASSWORD CRACKING

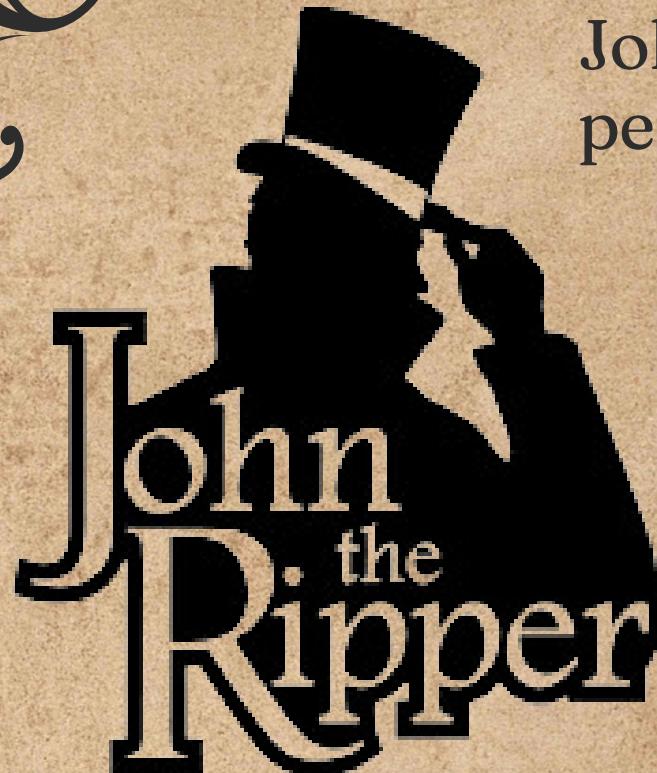
# TRACCIA

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

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

# JOHN THE RIPPER

John the Ripper è uno dei più popolari e potenti strumenti open-source per il password cracking.



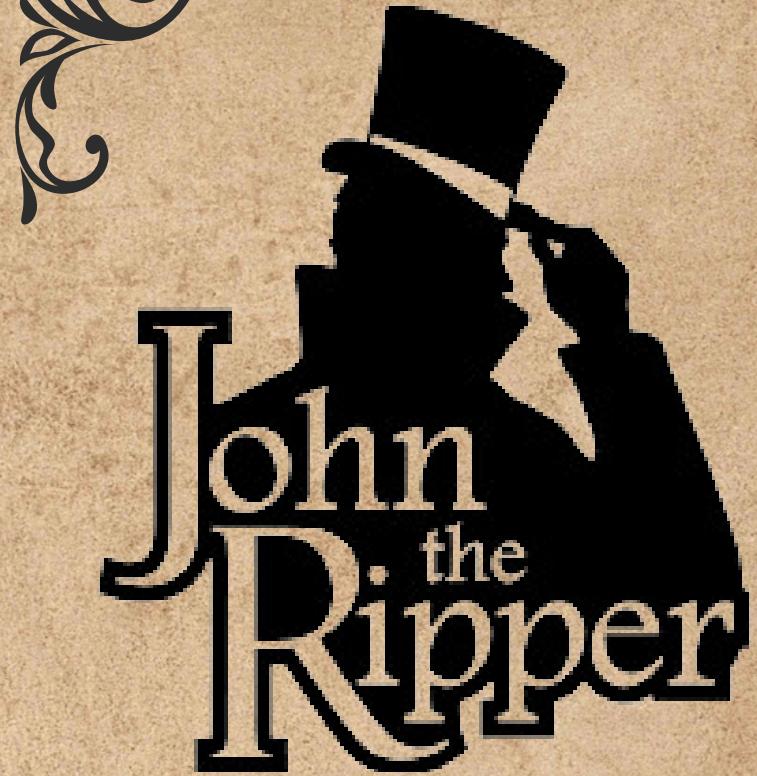
## Caratteristiche Principali

- **Multi-piattaforma:** Disponibile per Unix, macOS e Windows.
- **Supporto per vari formati di hash:** Può craccare password cifrate con diversi algoritmi come MD5, SHA-1, bcrypt, Kerberos, AFS, e molti altri.

## Diversi metodi di attacco:

- **Dictionary Attack:** Prova ogni parola in un elenco predefinito di parole.
- **Brute Force Attack:** Tenta ogni possibile combinazione di caratteri.
- **Incremental Mode:** Un tipo di brute force che può essere configurato per provare le combinazioni di caratteri in ordine di probabilità.

# JOHN THE RIPPER



```
(kali㉿kali)-[~/Desktop]
$ john --format=raw-md5 password.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])
No password hashes left to crack (see FAQ)

(kali㉿kali)-[~/Desktop]
$ john --show --format=raw-md5 password.txt
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left
```

# ALTRÉ STRUMENTI

- **Hashcat:** È uno degli strumenti più potenti e flessibili per il password cracking. Supporta una vasta gamma di algoritmi di hashing e può utilizzare sia il CPU che il GPU per craccare le password.
- **Hydra:** È uno strumento di password cracking molto versatile che può essere utilizzato per attacchi a forza bruta su vari protocolli di rete.
- **Cain & Abel:** Anche se un po' datato, è ancora molto usato per il cracking delle password su sistemi Windows.
- **RainbowCrack:** Utilizza le tabelle arcobaleno per accelerare il processo di cracking delle password.
- **Medusa:** Simile a Hydra, è uno strumento veloce e flessibile per il cracking delle password tramite attacchi a forza bruta.
- **Tool Online:** [link1](#), [link2](#)

```
(kali㉿kali)-[~]
$ rcrack . -l /home/kali/Desktop/ hashes.txt
1 rainbow tables found
memory available: 4934654361 bytes
memory for rainbow chain traverse: 16000 bytes per hash, 64000 bytes for 4 hashes
memory for rainbow table buffer: 2 x 16016 bytes
disk: ./md5_loweralpha-numeric#1-3_0_1000x1000_0.rt: 16000 bytes read
disk: finished reading all files
```

**MD5 Encrypt/Decrypt**

Share Add to Favs Report Bug

pepperstone Zero commissioni\*. Tutto oro. Sono \$0 di commissioni su ogni operazione. Fai trading sull'oro

\*Altri costi e spese potrebbero essere applicati. Il 75,8% dei conti degli investitori al dettaglio perdono denaro quando scambiano CFD con questo fornitore.

Encrypter Decrypter

MD5 Hash: 5f4dcc3b5aa765d61d8327deb882cf99

Text: password