PASSWORD CRACKING

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

Le password da craccare sono le seguenti:

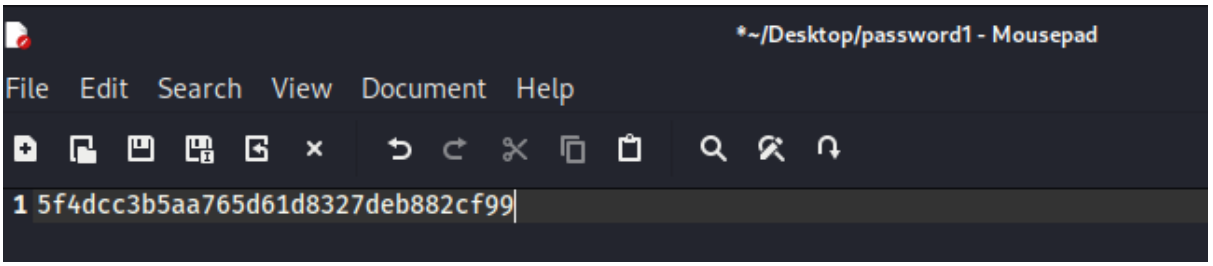
1) 5f4dcc3b5aa765d61d8327deb882cf99
2) e99a18c428cb38d5f260853678922e03
3) 8d3533d75ae2c3966d7e0d4fcc69216b
4) 0d107d09f5bbe40cade3de5c71e9e9b7
5) 5f4dcc3b5aa765d61d8327deb882cf99

Procedimento: Per questo password cracking si utilizzerà **John The Ripper.**

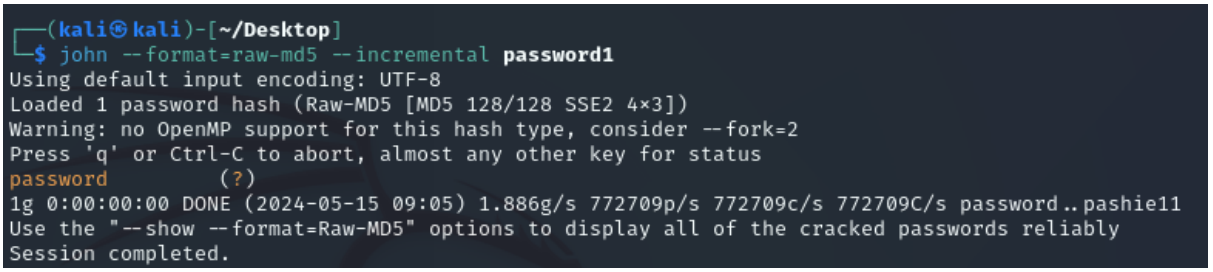
John The Ripper è un tool di password cracking, molto utile per gli attacchi di brute force alle password di file disponibili in loco, ovvero sullo stesso hardware in cui è installato John. Questo tool è altamente configurabile.

Iniziamo con la **password numero 1** (che è uguale alla password 5) ovvero 5f4dcc3b5aa765d61d8327deb882cf99.

Creiamo un file denominato password1 su desktop.



Apriamo la CLI di Kali e digitiamo il seguente comando: **"john --format=raw-md5 –incremental password1"**



Il comando utilizzato ci restituisce il valore alfanumerico di password1 ovvero **password.**

Abbiamo usato questo comando perché il parametro **–format=raw-md5** indica a John che la password da craccare si trova in un formato hash md5, poi con il parametro **–incremental** si fa in modo che John effettui un attacco incrementale. John creerà e testerà combinazioni di caratteri in modo sequenziale, partendo da una lunghezza minima preimpostata fino ad arrivare ad un riscontro o alla lunghezza massima preimpostata di caratteri. Quindi potrebbe partire da password di un singolo carattere, poi password di due caratteri e così via, aumentando sempre di più.

Utilizziamo lo stesso procedimento per le altre 4 password.

Password 2 = e99a18c428cb38d5f260853678922e03
Creiamo il file di testo, chiamiamolo password2 e immettiamo il comando di prima.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --format=raw-md5 --incremental password2
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4×3])
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           (?)
1g 0:00:00:00 DONE (2024-05-15 09:18) 3.703g/s 48355p/s 48355c/s 48355C/s amb100..abby99
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

La password in questo caso è **abc123**.

Password 3 = 8d3533d75ae2c3966d7e0d4fcc69216b
Creiamo il file di testo, chiamiamolo password3 e immettiamo il comando di prima.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --format=raw-md5 --incremental password3
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
charley          (?)
1g 0:00:00:00 DONE (2024-05-15 09:21) 4.545g/s 96872p/s 96872c/s 96872C/s stevy13..chertsu
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

La password in questo caso è **charley**.

Password 4 = 0d107d09f5bbe40cade3de5c71e9e9b7
Creiamo il file di testo, chiamiamolo password4 e immettiamo il comando di prima.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --format=raw-md5 --incremental password4
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
letmein          (?)
1g 0:00:00:00 DONE (2024-05-15 09:22) 1.219g/s 3114Kp/s 3114Kc/s 3114KC/s letebru..letmish
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

La password in questo caso è **letmein.**

Infine proviamo a vedere se John decifrerà tutte le password riunite in un singolo file.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --format=raw-md5 --incremental password
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4×3])
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 0:00:00:00 DONE (2024-05-15 09:46) 4.597g/s 2935Kp/s 2935Kc/s 3445KC/s letebru..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.
```

Come si vede, le ha decifrate tutte e 4 dato che password 1 e password 5 sono uguali.