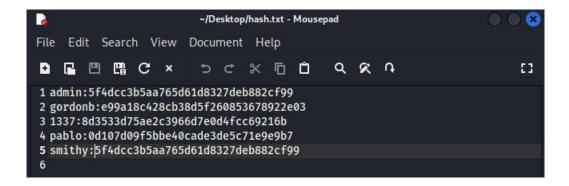
Per prima cosa, creiamo un file chiamato hash.txt nel quale andiamo ad immettere tutti gli user e le password estrapolate nella lezione precedente in questo formato: "user:password"



Dopodiché facciamo partire il tool John the ripper da terminale con l'opzione --format=raw-MD5 per specificare che si tratti di un hash md5 standard e puntandolo al file hash appena creato:

```
-(kali@kali)-[~/Desktop]
 $ sudo john --format=raw-MD5 /home/kali/Desktop/hash.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 256/256
AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 12 candidates buffered for the current salt, minimum 24
needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if
Proceeding with wordlist:/usr/share/john/password.lst
                (gordonb)
abc123
letmein
Proceeding with incremental:ASCII
charley
5g 0:00:00:01 DONE 3/3 (2024-02-28 05:35) 4.854g/s 176957p/s 176957c/s
193656C/s stevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracke
d passwords reliably
Session completed.
```

Come possiamo vedere il tool ha craccato le password con successo, volendo ottenere la lista completa delle password scoperte usiamo il parametro –show:

```
(kali@kali)-[~/Desktop]
$ sudo john --format=raw-MD5 /home/kali/Desktop/hash.txt --show
[sudo] password for kali:
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password
5 password hashes cracked, 0 left
```

È stato fatto un tentativo di decriptazione anche con Rainbow crack (tramite l'app rcracki\_mt) e delle tavole prese da Internet dalla dimensione di 24 GB

```
(kali® kali)-[~]
$ sudo rcracki_mt -l /home/kali/Desktop/hashes /media/sf_Shared/MD5
Using 1 threads for pre-calculation and false alarm checking...
Found 64 rainbowtable files...

md5_hybrid2(loweralpha#7-7,numeric#1-3)#0-0_0_15000×21854468_distrrtgen[p][i]_15.rti2
Chain Position is now 21854468
131126808 bytes read, disk access time: 5.86s
searching for 4 hashes...
☐ re-calculating hash 2 of 4.
```

Ma i risultati non sono stati soddisfacenti:

```
kali@kali: ~
 File Actions Edit View Help
cryptanalysis time: 1.46 s
md5_hybrid2(loweralpha#7-7,numeric#1-3)#0-0_3_15000×67108864_distrrtgen[p][i]_14.rti2
Chain Position is now 33870034
203220204 bytes read, disk access time: 4.09s
searching for 4 hashes...
cryptanalysis time: 1.43 s
Chain Position is now 67108864
199432980 bytes read, disk access time: 5.07s
searching for 4 hashes...
cryptanalysis time: 1.43 s
statistics
                                                                            0 of 4(0.00%)
plaintext found:
1799640016
5f4dcc3b5aa765d61d8327deb882cf99
e99a18c428cb38d5f260853678922e03
8d3533d75ae2c3966d7e0d4fcc69216b
                                                                        <notfound>
                                                                                                      hex:<notfound>
                                                                                                      hex:<notfound>
hex:<notfound>
                                                                         <notfound>
0d107d09f5bbe40cade3de5c71e9e9b7
5f4dcc3b5aa765d61d8327deb882cf99
                                                                         <notfound>
                                                                                                      hex:<notfound>
                                                                         <notfound>
```

Le tavole in questione non erano complete di tutti i caratteri presenti negli hash MD5, provando con tavole più complete si potrebbe arrivare ad un risultato positivo ma in questo caso il tool John the ripper è sicuramente più veloce ed efficiente.