

Creiamo files di testo corrispondenti agli hash che dobbiamo crackare.

```
(o@kali)-[~]
$ hashid -m 5f4dcc3b5aa765d61d8327deb882cf99
Analyzing '5f4dcc3b5aa765d61d8327deb882cf99'
[+] MD2
[+] MD5 [Hashcat Mode: 0]
[+] MD4 [Hashcat Mode: 900]
[+] Double MD5 [Hashcat Mode: 2600]
[+] LM [Hashcat Mode: 3000]
[+] RIPEMD-128
[+] Haval-128
[+] Tiger-128
[+] Skein-256(128)
[+] Skein-512(128)
[+] Lotus Notes/Domino 5 [Hashcat Mode: 8600]
[+] Skype [Hashcat Mode: 23]
[+] Snefru-128
[+] NTLM [Hashcat Mode: 1000]
[+] Domain Cached Credentials [Hashcat Mode: 1100]
[+] Domain Cached Credentials 2 [Hashcat Mode: 2100]
[+] DNSSEC(NSEC3) [Hashcat Mode: 8300]
[+] RAdmin v2.x [Hashcat Mode: 9900]
```

Attraverso `hashid` andiamo a capire che tipo di hash è quello che ci viene fornito.

```
- [ Hash modes ] -
```

| # | Name | Category |
|------|----------|----------|
| 900 | MD4 | Raw Hash |
| 0 | MD5 | Raw Hash |
| 100 | SHA1 | Raw Hash |
| 1300 | SHA2-224 | Raw Hash |
| 1400 | SHA2-256 | Raw Hash |

Possiamo vedere che il codice corrispondente a MD5 su Hashcat è 0.

```
(o@kali)-[~]  
$ hashcat -m 0 /home/o/Desktop/S6-L3/n1 -a 3  
hashcat (v6.2.6) starting
```

Andiamo a chiamare *hashcat*, con *-m* andiamo a specificare il tipo di hash che vogliamo crackare, inseriamo poi il path al file di testo dove si trova il nostro hash e con *-a* andiamo a specificare il tipo di attacco nel nostro caso *3* che corrisponde a un attacco brute-force.

```
5f4dcc3b5aa765d61d8327deb882cf99:password  
  
Session.....: hashcat  
Status.....: Cracked  
Hash.Mode.....: 0 (MD5)  
Hash.Target.....: 5f4dcc3b5aa765d61d8327deb882cf99  
Time.Started.....: Wed May 15 14:03:26 2024 (2 secs)  
Time.Estimated...: Wed May 15 14:03:28 2024 (0 secs)  
Kernel.Feature...: Pure Kernel  
Guess.Mask.....: ?1?2?2?2?2?2?2?3 [8]  
Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d*!$@_, -4 Undefined  
Guess.Queue.....: 8/15 (53.33%)  
Speed.#1.....: 931.7 MH/s (11.91ms) @ Accel:64 Loops:64 Thr:1024 Vec:1  
Speed.#2.....: 146.2 MH/s (14.24ms) @ Accel:256 Loops:1024 Thr:1 Vec:8  
Speed.#*.....: 1077.9 MH/s  
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)  
Progress.....: 2037317632/5533380698112 (0.04%)  
Rejected.....: 0/2037317632 (0.00%)  
Restore.Point....: 0/68864256 (0.00%)  
Restore.Sub.#1...: Salt:0 Amplifier:8896-8960 Iteration:0-64  
Restore.Sub.#2...: Salt:0 Amplifier:54272-55296 Iteration:0-1024  
Candidate.Engine.: Device Generator  
Candidates.#1....: 7zuerane -> 653k4800  
Candidates.#2....: 3dpo1723 -> E7gn6ama  
Hardware.Mon.#1..: Temp: 72c Util: 97% Core:1290MHz Mem:2504MHz Bus:4  
Hardware.Mon.#2..: Temp: 74c Util: 94%  
  
Started: Wed May 15 14:01:17 2024  
Stopped: Wed May 15 14:03:30 2024
```

e99a18c428cb38d5f260853678922e03:abc123

```
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 0 (MD5)
Hash.Target.....: e99a18c428cb38d5f260853678922e03
Time.Started.....: Wed May 15 14:06:27 2024 (0 secs)
Time.Estimated...: Wed May 15 14:06:27 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.....: ?1?2?2?2?2?2 [6]
Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d*!$@_, -4 Undefined
Guess.Queue.....: 6/15 (40.00%)
Speed.#1.....: 0 H/s (12.60ms) @ Accel:32 Loops:128 Thr:1024 Vec:1
Speed.#2.....: 175.8 MH/s (11.30ms) @ Accel:512 Loops:512 Thr:1 Vec:8
Speed.#*.....: 175.8 MH/s
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 2097152/3748902912 (0.06%)
Rejected.....: 0/2097152 (0.00%)
Restore.Point....: 0/1679616 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-128 Iteration:0-128
Restore.Sub.#2...: Salt:0 Amplifier:0-512 Iteration:0-512
Candidate.Engine.: Device Generator
Candidates.#1....: sa6588 -> coby25
Candidates.#2....: sanier -> hshian
Hardware.Mon.#1..: Temp: 58c Util: 94% Core:1139MHz Mem:2504MHz Bus:4
Hardware.Mon.#2..: Temp: 65c Util: 19%
```

Started: Wed May 15 14:06:22 2024

Stopped: Wed May 15 14:06:28 2024

8d3533d75ae2c3966d7e0d4fcc69216b:charley

```
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 0 (MD5)
Hash.Target.....: 8d3533d75ae2c3966d7e0d4fcc69216b
Time.Started.....: Wed May 15 14:09:33 2024 (16 secs)
Time.Estimated...: Wed May 15 14:09:49 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.....: ?1?2?2?2?2?2?2 [7]
Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d*!$@_, -4 Undefined
Guess.Queue.....: 7/15 (46.67%)
Speed.#1.....: 979.2 MH/s (11.37ms) @ Accel:32 Loops:128 Thr:1024 Vec:1
Speed.#2.....: 159.1 MH/s (15.43ms) @ Accel:256 Loops:1024 Thr:1 Vec:8
Speed.#*.....: 1138.2 MH/s
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 18377408512/134960504832 (13.62%)
Rejected.....: 0/18377408512 (0.00%)
Restore.Point....: 217088/1679616 (12.92%)
Restore.Sub.#1...: Salt:0 Amplifier:0-128 Iteration:0-128
Restore.Sub.#2...: Salt:0 Amplifier:48128-49152 Iteration:0-1024
Candidate.Engine.: Device Generator
Candidates.#1....: sar3qvy -> cons775
Candidates.#2....: gfp5c60 -> Kajgqvy
Hardware.Mon.#1..: Temp: 64c Util: 95% Core:1265MHz Mem:2504MHz Bus:4
Hardware.Mon.#2..: Temp: 66c Util: 94%
```

Started: Wed May 15 14:09:25 2024

Stopped: Wed May 15 14:09:51 2024

0d107d09f5bbe40cade3de5c71e9e9b7:letmein

```
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 0 (MD5)
Hash.Target.....: 0d107d09f5bbe40cade3de5c71e9e9b7
Time.Started.....: Wed May 15 14:10:12 2024 (2 secs)
Time.Estimated...: Wed May 15 14:10:14 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.....: ?1?2?2?2?2?2 [7]
Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d*!$@_, -4 Undefined
Guess.Queue.....: 7/15 (46.67%)
Speed.#1.....: 924.7 MH/s (12.31ms) @ Accel:32 Loops:128 Thr:1024 Vec:1
Speed.#2.....: 211.3 MH/s (9.64ms) @ Accel:256 Loops:1024 Thr:1 Vec:8
Speed.#*.....: 1136.1 MH/s
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 1653538816/134960504832 (1.23%)
Rejected.....: 0/1653538816 (0.00%)
Restore.Point....: 0/1679616 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:13568-13696 Iteration:0-128
Restore.Sub.#2...: Salt:0 Amplifier:69632-70656 Iteration:0-1024
Candidate.Engine.: Device Generator
Candidates.#1....: Isiwrin -> V15g242
Candidates.#2....: 06v3a10 -> Cn7mahe
Hardware.Mon.#1..: Temp: 64c Util: 86% Core:1189MHz Mem:2504MHz Bus:4
Hardware.Mon.#2..: Temp: 77c Util: 86%

Started: Wed May 15 14:10:04 2024
Stopped: Wed May 15 14:10:16 2024
```

Possiamo vedere che abbiamo ottenuto in pochi secondi tutte le password.