

Cracking Password

Per questo esercizio i tool che sono stati utilizzati per effettuare il cracking sono: **John the ripper** e **Hashcat**.

```
kali@kali: ~  
File Actions Edit View Help  
$ john  
Created directory: /home/kali/.john  
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 OMP [linux-gnu  
64-bit x86_64 SSE2 AC]  
Copyright (c) 1996-2021 by Solar Designer and others  
Homepage: https://www.openwall.com/john/  
Usage: john [OPTIONS] [PASSWORD-FILES] [HASH-FILES] [TIME-OUT] [MACHINE]  
Use --help to list all available options.  
zsh: corrupt history file /home/kali/.zsh_history  
(kali@kali)-[~]  
$ sudo nano  
[sudo] password for kali:  
(kali@kali)-[~]  
$ john --format=RAW-MD5 hash.txt  
Using default input encoding: UTF-8  
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])  
Warning: no OpenMP support for this hash type, consider --fork=3  
Proceeding with single, rules:Single  
Press 'q' or Ctrl-C to abort, almost any other key for status  
Almost done: Processing the remaining buffered candidate passwords, if any.  
Proceeding with wordlist:/usr/share/john/password.lst  
password (?)  
password (?)  
abc123 (?)  
letmein (?)  
Proceeding with incremental:ASCII  
charley (?)  
5g 0:00:00:00 DONE 3/3 (2024-07-03 06:30) 9.615g/s 342611p/s 342611c/s 344088C/s stevy13..chertsu  
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably  
Session completed.  
(kali@kali)-[~]  
$
```

```
kali@kali: ~/Desktop  
File Firefox ESR Browse the World Wide Web  
Initializing device kernels and memory. Please be patient ... Initializing backend runtime for device #1. Please be patient ... Initialized backend runtime for device #1Host memory required f  
or this attack: 0 MB  
Initialized device kernels and memoryStarting self-test. Please be patient ... Finished self-testDictionary cache building rockyou.txt: 33553434 bytes (23.98%)Dictionary cache building rock  
you.txt: 100660302 bytes (71.94%)Dictionary cache built:  
* Filename..: rockyou.txt  
* Passwords.: 14344392  
* Bytes.....: 139921507  
* Keyspace..: 14344385  
* Runtime...: 1 sec  
5f4dcc3b5aa765d61d8327deb882cf90:password  
e99a18c428cb38d5f260852678922e03:abc123  
0d107d09f5bbe40cade3de5c71e9e9b7:letmein  
8d3533d75ae2c3966d7e0d4fcc69216b:charley  
Session.....: hashcat  
Status.....: Cracked  
Hash.Mode.....: 0 (MD5)  
Hash.Target.....: hash.txt  
Time.Started.....: Wed Jul 3 08:54:16 2024 (0 secs)  
Time.Estimated...: Wed Jul 3 08:54:16 2024 (0 secs)  
Kernel.Feature...: Pure Kernel  
Guess.Base.....: File (rockyou.txt)  
Guess.Queue.....: 1/1 (100.00%)  
Speed.#1.....: 23852 H/s (0.13ms) @ Accel:256 Loops:1 Thr:1 Vec:4  
Recovered.....: 4/4 (100.00%) Digests (total), 4/4 (100.00%) Digests (new)  
Progress.....: 3072/14344385 (0.02%)  
Rejected.....: 0/3072 (0.00%)  
Restore.Point...: 2304/14344385 (0.02%)  
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1  
Candidate.Engine.: Device Generator  
Candidates.#1....: skyblue -> dangerous  
Hardware.Mon.#1..: Util: 36%  
Started: Wed Jul 3 08:53:27 2024  
Stopped: Wed Jul 3 08:54:18 2024
```