kali@kali: ~/Desktop
File Actions Edit View Help
┌──(kali㉿kali)-[~/Desktop]
└─$ john DVWA.txt --format=Raw-MD5
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 5 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
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 (2023-03-01 09:37) 17.85g/s 636278p/s 636278c/s 639021C/s stevy13..chertsu
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
┌──(kali㉿kali)-[~/Desktop]
└─$
KALI LINUX
the quieter you become, the more you are able to hear"

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
5f4dcc3b5aa765d61d8327deb882cf99
e99a18c428cb38d5f260853678922e03
8d3533d75ae2c3966d7e0d4fcc69216b
0d107d09f5bbe40cade3de5c71e9e9b7
5f4dcc3b5aa765d61d8327deb882cf99
```

Non sono un robot

reCAPTCHA
Privacy - Termini

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
5f4dcc3b5aa765d61d8327deb882cf99	md5	password
e99a18c428cb38d5f260853678922e03	md5	abc123
8d3533d75ae2c3966d7e0d4fcc69216b	md5	charley
0d107d09f5bbe40cade3de5c71e9e9b7	md5	letmein
5f4dcc3b5aa765d61d8327deb882cf99	md5	password

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

*~/Desktop/Password.txt - Mousepad

File Edit Search View Document Help

```
1 5f4dcc3b5aa765d61d8327deb882cf99:password
2 e99a18c428cb38d5f260853678922e03:abc123
3 0d107d09f5bbe40cade3de5c71e9e9b7:letmein
4 8d3533d75ae2c3966d7e0d4fcc69216b:charley
5 `
```

DVWA.txt

Password.txt

kali@kali: ~/Desktop

File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Desktop]
└─$ hashcat -m 0 -a 0 DVWA.txt /usr/share/wordlists/rockyou.txt -o Password.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 3.1+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 14.0.6, SLEEF, DISTRO, POCL_DEBUG) -
 Platform #1 [The pocl project]
═══════════════════════════════════════════════════════════════════════════════
* Device #1: pthread-penryn-Intel(R) Core(TM) i5-7600K CPU @ 3.80GHz, 2141/4347 MB (1024 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 5 digests; 4 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0×0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 1 sec


Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: DVWA.txt
Time.Started.....: Wed Mar  1 09:44:42 2023 (0 secs)
Time.Estimated...: Wed Mar  1 09:44:42 2023 (0 secs)
Kernel.Feature...: Pure Kernel
```