

# тулзы для pwd cracking

СПИСОК ОСНОВНЫХ ИНСТРУМЕНТОВ для решения задач

# ОСНОВНЫЕ ПОНЯТИЯ

- › хэш-функции — это функции, предназначенные для «сжатия» произвольного сообщения или набора данных, записанных, как правило, в двоичном алфавите, в некоторую битовую комбинацию фиксированной длины, называемую сверткой
- › статья 272
- › статья 137
- › брут — метод взлома путем подбора паролей. суть подхода заключается в последовательном автоматизированном переборе всех возможных комбинаций символов с целью рано или поздно найти правильную.
- › соль — строка данных, которая передаётся хеш-функции вместе с входным массивом данных для вычисления хэша

ХЭШН

```
> hash-identifier
```

скрипт `hash-identifier` позволяет определить тип любых хэшей, чтобы затем указать правильный режим при работе с Hashcat.

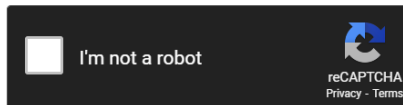
[illegible]

# > crackstation.net

## Free Password Hash Cracker

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

a64ed26872a12b34a54f97e893a2161a



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
a64ed26872a12b34a54f97e893a2161a	md5	iwannasleep

сайт пробивает хэши поддерживаемых форматов по своим вордлистам, определяя наиболее вероятный формат и, в случае нахождения данных, передает первообразную от хэша

› ворддлусты

- › rockyou.txt
- › google-10000-english
- › crackstation's password cracking dictionary
- › hashesorg
- › weakpass
- › dchtpassv1.0.txt

› тулзы для перебора



# > john the ripper

```
root@yos: ~  
root@yos:~# john  
John the Ripper 1.9.0-jumbo-1 OMP [linux-gnu 64-bit x86_64 AVX2 AC]  
Copyright (c) 1996-2019 by Solar Designer and others  
Homepage: http://www.openwall.com/john/  
  
Usage: john [OPTIONS] [PASSWORD-FILES]  
--single[=SECTION[,...]] "single crack" mode, using default or named rules  
--single=:rule[,...] same, using "immediate" rule(s)  
--wordlist[=FILE] --stdin wordlist mode, read words from FILE or stdin  
--pipe like --stdin, but bulk reads, and allows rules  
--loopback[=FILE] like --wordlist, but extract words from a .pot file  
--dupe-suppression suppress all dupes in wordlist (and force preload)  
--prince[=FILE] PRINCE mode, read words from FILE  
--encoding=NAME input encoding (eg. UTF-8, ISO-8859-1). See also  
doc/ENCODINGS and --list=hidden-options.  
--rules[=SECTION[,...]] enable word mangling rules (for wordlist or PRINCE  
modes), using default or named rules  
--rules=:rule[;...]] same, using "immediate" rule(s)  
--rules-stack=SECTION[,...] stacked rules, applied after regular rules or to  
modes that otherwise don't support rules  
--rules-stack=:rule[;...]] same, using "immediate" rule(s)  
--incremental[=MODE] "incremental" mode [using section MODE]  
--mask[=MASK] mask mode using MASK (or default from john.conf)  
--markov[=OPTIONS] "Markov" mode (see doc/MARKOV)  
--external=MODE external mode or word filter  
--subsets[=CHARSET] "subsets" mode (see doc/SUBSETS)  
--stdout[=LENGTH] just output candidate passwords [cut at LENGTH]  
--restore[=NAME] restore an interrupted session [called NAME]  
--session=NAME give a new session the NAME  
--status[=NAME] print status of a session [called NAME]  
--make-charset=FILE make a charset file. It will be overwritten
```

john the ripper проводит атаку по словарю и брутфорс. в режиме атаки по словарю программа берёт предполагаемые пароли из указанного файла, генерирует хеш и сверяет его с эталонным. в режиме брутфорса программа перебирает все возможные комбинации пароля.

# > hashcat

```
root@yos: ~  
root@yos:~# hashcat --help  
hashcat (v6.1.1) starting...  
  
Usage: hashcat [options]... hash[hashfile|hccapxfile [dictionary|mask|directory]...  
  
- [ Options ] -  
  
Options Short / Long      | Type | Description  
| Example  
=====+=====+=====+  
-m, --hash-type           | Num  | Hash-type, see references below  
| -m 1000  
-a, --attack-mode         | Num  | Attack-mode, see references below  
| -a 3  
-V, --version             |      | Print version  
-h, --help                |      | Print help  
--quiet                   |      | Suppress output  
--hex-charset              |      | Assume charset is given in hex  
--hex-salt                 |      | Assume salt is given in hex  
--hex-wordlist             |      | Assume words in wordlist are given in hex  
--force                    |      | Ignore warnings  
--status                  |      | Enable automatic update of the status screen  
--status-json              |      | Enable JSON format for status output
```

особенностью hashcat является очень высокая скорость перебора паролей, которая достигается благодаря одновременному использованию всех видео карт, а также процессоров в системе.

» демо

# » demo

- › дан запароленный архив и строка '215f6ca4fc913f15ff882e3531c8435d'
- › понимаем, что это хэш
- › пробиваем его на crackstation

Hash	Type	Result
215f6ca4fc913f15ff882e3531c8435d	md5	Wizard\$619

- › получаем пароль от архива
- › внутри архива есть file.txt, открываем его

```
dCBkawQgZ2l2ZSB0aGUgZGFya251c3MgYSBzaGFwZeKApgok4oCcT2gsIG5v4oCdIGHlIGJyZWFOaGVkLgoKQ1VUIF1FUywg2FpZCBEZWFOaC4KC1JpbmNld2luZCByb2xsZWQuID
Roc2wzM3B7dzB3XzF0X3c0c19oNHNoIX0KCkZvc1BhIG1vbWVudCBoZSB0aG91Z2h0IFdpdGhlbCB3YXMGZ29pbmcgdG8gc3BpdCBoaw0gd2hlcmUgaGUgbGF5LiBCdXQgaXQgd2Fz
IHdvcnNlIHROyW4gdGhhc4gSGUgd2FzIHdhaXRpbmcgZm9yIGhpbSB0byBnZXQgdXAuCGrigJxJIHNlZSB5b3UgaGF2ZSBhIHN3b3JkLCB3aXphcmQs4oCdIGHlIHNhawQgcXVpZX
RseS4g4oCcSSBzdWdnZXN0IHlvdSByaXNlLCBhbmQgd2Ugc2hhbGwgc2VlIGhvdYB3ZWxsIHlvdSB1c2UgaXQu4oCdIFJpbmNld2luZCByb29vZCBlcCBhcyBzbG93bHkgYXMGaGUg
ZGFyZWQsIGFuZCBlcmV3IGZyb20gaGlzIGJlbH0gdGhlIHNob3J0IHN3b3JkIGHlIGhhZCB0YWt1biBmcm9tIHRoZSBndWFyZCBlIGZldyBob3VycyBhbmQgYSBodW5kcmVkiH1lYX
```

- › текст в какой-то кодировке
- › декодируем его через cybershef
- › находим флаг