HASHCAT [PASSWORD CRACKING]

Contributor:
JON GORENFLO @flakpaket

Basic Syntax

```
hashcat [options]... hash|hashfile|hccapxfile
[dictionary|mask|directory]...
```

Searching for Options

Unix

```
hashcat --help | grep -i [string]
```

Windows

```
hashcat --help | find /i "[string]"
```

Attack Modes

#	Mode	Description
0	Straight	Dictionary Attack
1	Combination	Uses 2 wordlists, each word in list 2 is appended to each word in list 1
3	Brute-force	Use Masks, Markov, or pure brute force
6	Hybrid Wordlist + Mask	Like Combination, but uses a wordlist and brute force
7	Hybrid Mask + Wordlist	Like Combination, but uses brute force and a wordlist

Common Hash Modes

RAW

#	Name
0	MD5
100	SHA1
1400	SHA-256
1700	SHA-512

ARCHIVES

#	Name
11600	7-Zip
13600	WinZip
12500	RAR3-hp
13000	RAR5
14800	iTunes backup >= 10.0

OPERATING SYSTEMS

#	Name
1000	NTLM
3000	LM
1100	Domain Cached Credentials (DCC), MS Cache
2100	Domain Cached Credentials 2 (DCC2), MS Cache 2
12800	MS-AzureSync PBKDF2-HMAC-SHA256
5700	Cisco-IOS type 4 (SHA256)
9200	Cisco-IOS (PBKDF2-SHA256)
9300	Cisco-IOS (scrypt)
1500	descrypt, DES (Unix), Traditional DES
7400	sha256crypt, SHA256 (Unix)
1800	sha512crypt, SHA512 (Unix)

NETWORK PROTOCOLS

#	Name
5500	NetNTLMv1
5500	NetNTLMv1+ESS
5600	NetNTLMv2
7500	Kerberos 5 AS-REQ Pre-Auth etype 23
2500	WPA/WPA2
2501	WPA/WPA2 PMK
5300	IKE-PSK MD5
5400	IKE-PSK SHA1

WEB PLATFORMS

#	Name
400	Wordpress, Joomla >= 2.5.18 (MD5)
7900	Drupal7
124	Django (SHA-1)
10000	Django (PBKDF2-SHA256)
3711	MediaWiki B type

DATABASES

#	Name
11200	MySQL CRAM (SHA1)
200	MySQL323
300	MySQL4.1/MySQL5
112	Oracle S: Type (Oracle 11+)
12300	Oracle T: Type (Oracle 12+)
1731	MSSQL (2012, 2014)
11100	PostgreSQL CRAM (MD5)

DOCUMENTS

#	Name
9400	MS Office 2007
9500	MS Office 2010
600	MS Office 2013
10600	PDF 1.7 Level 3 (Acrobat 9)
10700	PDF 1.7 Level 8 (Acrobat 10 - 11)

Generate Wordlists for Other Tools with --stdout

hashcat -a 3 --stdout Password?d | Creates list: Password0-Password9

hashcat -a 6 --stdout wordlist.dic ?d | Append digits to the end of words

hashcat -a 7 --stdout ?d wordlist.dic | Prepent digits to the beginning of words

Performance Tweaks

-O | (Capital 'O') Optimize Kernel, Passwords < 32 Char.

-w [#]

#	Performance
1	Low
2	Default
3	High
4	Nightmare

```
hashcat -w 3 -O -a 0 -m [#] [hashfile] [wordlist]
```

Examples

Straight

```
hashcat -a 0 -m [#] [hashfile] [wordlist]
hashcat -a 0 -m [#] [hashfile] [wordlist] -r [rulefile]
```

Brute-force

```
hashcat -a 3 -m [#] [hashfile]
hashcat -a 3 -m [#] [hashfile] [mask]
```

Hybrid Wordlist + Mask

```
hashcat -a 6 -m [#] [hashfile] [wordlist] [mask]
```

Hybrid Mask + Wordlist

```
hashcat -a 7 -m [#] [hashfile] [mask] [wordlist]
```

Combination

```
hashcat -a 1 -m [#] [hashfile] [wordlist-1] [wordlist-2]
hashcat -a 1 -m [#] [hashfile] [wordlist-1] [wordlist-2] -j [rule] -k [rule]
```

	Rules Description
$	Append characters
^	Prepend characters
c	Capitalize first letter, lower the rest
t	Toggle case for all characters
d	Duplicate entire word
l	Lowercase all letters
u	Uppercase all letters
r	Reverse the word

Info Commands

hashcat -I | Show info about OpenCL devices

hashcat -b | Benchmark all hashes

hashcat -b -m [#] | Benchmark a specific hash mode

hashcat -V | Show Verion info

hashcat [hashfile] --show | Show cracked hashes

hashcat [hashfile] --left | Show uncracked hashes

Built-in Character Sets

Character sets are combined to create "masks" or patterns for brute force attacks.

Mask	Characters
?l	abcdefghijklmnopqrstuvwxyz
?u	ABCDEFGHIJKLMNOPQRSTUVWXYZ
?d	0123456789
?h	0123456789abcdef
?H	0123456789ABCDEF
?s	«space»!"#$%&'()*+,-./:;<=>?@[]^_`{|}~
?a	?l?u?d?s
?b	0x00 - 0xff