Hashcat 4.10 Cheat Sheet v.2018.1b

@BHInfoSecurity @Krelkci

https://www.blackhillsinfosec.com

https://hashcat.net/hashcat/
https://github.com/hashcat/hashcat

Hash Types (-m)

RAW HASH

900	MD4
0	MD5
5100	Half MD5
100	SHA1
1300	SHA-224
1400	SHA-256
10800	SHA-384
1700	SHA-512
5000	SHA-3 (Keccak)
600	BLAKE2b-512
10100	SipHash
6000	RIPEMD-160
6100	Whirlpool
6900	GOST R 34.11-94
11700	GOST R 34.11-2012 (Streebog) 256-bit
11800	GOST R 34.11-2012 (Streebog) 512-bit

RAW HASH + SALT / ITERATION **

10	md5($pass.$salt)
20	md5($salt.$pass)
30	md5(utf16le($pass).$salt)
40	md5($salt.utf16le($pass))
3800	md5($salt.$pass.$salt)
3710	md5($salt.md5($pass))
4010	md5($salt.md5($salt.$pass))
4110	md5($salt.md5($pass.$salt))
2600	md5(md5($pass))
3910	md5(md5($pass).md5($salt))
4300	md5(strtoupper(md5($pass)))
4400	md5(sha1($pass))
110	sha1($pass.$salt)
120	sha1($salt.$pass)
130	sha1(utf16le($pass).$salt)
140	sha1($salt.utf16le($pass))
4500	sha1(sha1($pass))
4520	sha1($salt.sha1($pass))
4700	sha1(md5($pass))
4900	sha1($salt.$pass.$salt)
14400	sha1(CX)
1410	sha256($pass.$salt)
1420	sha256($salt.$pass)
1430	sha256(utf16le($pass).$salt)
1440	sha256($salt.utf16le($pass))
1710	sha512($pass.$salt)
1720	sha512($salt.$pass)
1730	sha512(utf16le($pass).$salt)
1740	sha512($salt.utf16le($pass))

***RAW HASH, AUTHENTICATED ***

50	HMAC-MD5 (key = $pass)
60	HMAC-MD5 (key = $salt)
150	HMAC-SHA1 (key = $pass)
160	HMAC-SHA1 (key = $salt)
1450	HMAC-SHA256 (key = $pass)
1460	HMAC-SHA256 (key = $salt)
1750	HMAC-SHA512 (key = $pass)
1760	HMAC-SHA512 (key = $salt)

*** RAW CIPHER, KNOWN ATTACK ***

14000	DES (PT = $salt, key = $pass)
14100	3DES (PT = $salt, key = $pass)
14900	Skip32 (PT = $salt, key = $pass)
15400	ChaCha20

*** GENERIC KDF***

400	phpass
8900	scrypt
11900	PBKDF2-HMAC-MD5
12000	PBKDF2-HMAC-SHA1
10900	PBKDF2-HMAC-SHA256
12100	PBKDF2-HMAC-SHA512

*** NETWORK PROTOCOLS ***

23	Skype
2500	**WPA/WPA2**
2501	**WPA/WPA2 PMK**
4800	iSCSI CHAP authentication, MD5(CHAP)
5300	IKE-PSK MD5
5400	IKE-PSK SHA1
5500	**NetNTLMv1**
5500	**NetNTLMv1+ESS**
5600	**NetNTLMv2**
7300	IPMI2 RAKP HMAC-SHA1
7500	**Kerberos 5 AS-REQ Pre-Auth etype 23**
8300	DNSSEC (NSEC3)
10200	CRAM-MD5
11100	PostgreSQL CRAM (MD5)
11200	**MySQL CRAM (SHA1)**
11400	SIP digest authentication (MD5)
13100	**Kerberos 5 TGS-REP etype 23**
16100	TACACS+
16500	JWT (JSON Web Token)

*** FORUMS ***

121	SMF (Simple Machines Forum) > v1.1
400	phpBB3 (MD5)
2611	vBulletin < v3.8.5
2711	vBulletin >= v3.8.5
2811	MyBB 1.2+
2811	IPB2+ (Invision Power Board)
8400	WBB3 (Woltlab Burning Board)

*** CONTENT MANAGEMENT SYSTEMS ***

11	Joomla < 2.5.18
400	Joomla >= 2.5.18 (MD5)
400	**WordPress (MD5)**
2612	PHPS
7900	Drupal7

*** COMMERCE, FRAMEWORKS ***

21	osCommerce
21	xt:Commerce
11000	PrestaShop
124	Django (SHA-1)
10000	Django (PBKDF2-SHA256)
16000	Tripcode
3711	MediaWiki B type
13900	OpenCart
4521	Redmine
4522	PunBB
12001	Atlassian (PBKDF2-HMAC-SHA1)

*** DATABASE SERVERS ***

12	**PostgreSQL**
131	MSSQL (2000)
132	MSSQL (2005)
1731	**MSSQL (2012, 2014)**
200	MySQL323
300	**MySQL4.1/MySQL5**
3100	Oracle H: Type (Oracle 7+)
112	Oracle S: Type (Oracle 11+)
12300	Oracle T: Type (Oracle 12+)
8000	Sybase ASE

*** HTTP, SMTP, LDAP, FTP ***

141	Episerver 6.x < .NET 4
1441	Episerver 6.x >= .NET 4
1600	**Apache $apr1$ MD5, md5apr1, MD5 ARP**
12600	ColdFusion 10+
1421	hMailServer
101	nsldap, SHA-1(Base64), Netscape LDAP SHA
111	nsldaps, SSHA-1(Base64), Netscape LDAP SSHA
1411	SSHA-256(Base64), LDAP {SSHA256}
1711	SSHA-512(Base64), LDAP {SSHA512}
16400	CRAM-MD5 Dovecot
15000	FileZilla Server >= 0.9.55

*** CHECKSUM ***

11500	CRC32

*** OPERATING SYSTEMS ***

3000	**LM**
1000	**NTLM**
1100	**Domain Cached Credentials (DCC), MS Cache**
2100	**Domain Cached Credentials 2 (DCC2), MS Cache 2**
15300	DPAPI masterkey file v1
15900	DPAPI masterkey file v2
12800	MS-AzureSync PBKDF2-HMAC-SHA256
1500	descrypt, DES (Unix), Traditional DES
12400	BSDi Crypt, Extended DES
500	md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5)
3200	bcrypt $2*$, Blowfish (Unix)
7400	sha256crypt $5$, SHA256 (Unix)
1800	ha512crypt $6$, SHA512 (Unix)
122	macOS v10.4, MacOS v10.5, MacOS v10.6
1722	macOS v10.7
7100	**macOS v10.8+ (PBKDF2-SHA512**)
6300	AIX {smd5}
6700	AIX {ssha1}
6400	AIX {ssha256}
6500	AIX {ssha512}
2400	Cisco-PIX MD5
2410	Cisco-ASA MD5
500	Cisco-IOS $1$ (MD5)
5700	Cisco-IOS type 4 (SHA256)
9200	Cisco-IOS $8$ (PBKDF2-SHA256)
9300	**Cisco-IOS $9$ (scrypt)**
22	Juniper NetScreen/SSG (ScreenOS)
501	Juniper IVE
15100	Juniper/NetBSD sha1crypt
7000	**FortiGate (FortiOS)**
5800	Samsung Android Password/PIN
13800	Windows Phone 8+ PIN/password
8100	Citrix NetScaler
8500	RACF
7200	GRUB 2
9900	Radmin2
125	ArubaOS

*** ENTERPRISE APPLICATION SOFTWARE ***

7700	SAP CODVN B (BCODE)
7800	SAP CODVN F/G (PASSCODE)
10300	SAP CODVN H (PWDSALTEDHASH) iSSHA-1
8600	Lotus Notes/Domino 5
8700	Lotus Notes/Domino 6
9100	Lotus Notes/Domino 8
133	PeopleSoft
13500	PeopleSoft PS_TOKEN

*** ARCHIVES ***

11600	**7-Zip**
12500	RAR3-hp
13000	RAR5
13200	AxCrypt
13300	AxCrypt in-memory SHA1
13600	**WinZip**

*** BACKUP ***

14700	iTunes backup < 10.0
14800	iTunes backup >= 10.0

*** FULL DISK ENCRYPTION ***

62XY	**TrueCrypt**
8800	Android FDE <= 4.3
12900	Android FDE (Samsung DEK)
12200	eCryptfs
137XY	VeraCrypt
14600	**LUKS**

*** DOCUMENTS ***

9700	MS Office <= 2003 $0/$1, MD5 + RC4
9710	MS Office <= 2003 $0/$1, MD5 + RC4, collider #1
9720	MS Office <= 2003 $0/$1, MD5 + RC4, collider #2
9800	MS Office <= 2003 $3/$4, SHA1 + RC4
9810	MS Office <= 2003 $3, SHA1 + RC4, collider #1
9820	MS Office <= 2003 $3, SHA1 + RC4, collider #2
9400	**MS Office 2007**
9500	**MS Office 2010**
9600	**MS Office 2013**
10400	PDF 1.1 - 1.3 (Acrobat 2 - 4)
10410	PDF 1.1 - 1.3 (Acrobat 2 - 4), collider #1
10420	PDF 1.1 - 1.3 (Acrobat 2 - 4), collider #2
10500	PDF 1.4 - 1.6 (Acrobat 5 - 8)
10600	PDF 1.7 Level 3 (Acrobat 9)
10700	PDF 1.7 Level 8 (Acrobat 10 - 11)
16200	Apple Secure Notes

*** PASSWORD MANAGERS ***

9000	Password Safe v2
5200	Password Safe v3
6800	**LastPass + LastPass sniffed**
6600	1Password, agilekeychain
8200	1Password, cloudkeychain
11300	Bitcoin/Litecoin wallet.dat
12700	Blockchain, My Wallet
15200	Blockchain, My Wallet, V2
16600	Electrum Wallet (Salt-Type 1-3)
13400	KeePass 1 (AES/Twofish) and KeePass 2 (AES)
15500	JKS Java Key Store Private Keys (SHA1)
15600	Ethereum Wallet, PBKDF2-HMAC-SHA256
15700	Ethereum Wallet, SCRYPT
16300	Ethereum Pre-Sale Wallet, PBKDF2-HMAC-SHA256

*** PLAIN TEXT ***

9999	Plaintext

Attack Modes

-a 0	Straight	[hash] [dictionary]
-a 1	Combination	[hash] [dictionary] [dictionary]
-a 3	Brute-Force	[hash] [mask]
-a 6	Hybrid Wordlist + Mask	[hash] [dictionary] [mask]
-a 7	Hybrid Mask + Wordlist	[hash] [dictionary] [mask]

Character Sets (Default) [?]

?l	abcdefghijklmnopqrstuvwxyz	[26]
?u	ABCDEFGHIJKLMNOPQRSTUVWXYZ	[26]
?d	0123456789	[10]
?h	0123456789abcdef	[16]
?H	0123456789ABCDEF	[16]
?s	!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~	[33]
?a	?l?u?d?s	[95]
?b	0x00 - 0xff	[255]

Device Types (-D)

-D 1	CPU
-D 2	GPU
-D 3	FPGA, DSP, Co-Proc

Options

-m [#]	Hash Type (mode)
-a [#]	Attack Mode
-r [file]	Rules file
-V	Version
--status	Keep screen updated
-b	Benchmark
--runtime [#]	Abort after x seconds
--session [text]	Set session name (resumeable)
--restore	Restore/Resume session
-o [filename]	Define output/potfile
--username	Ignore username field in hashfile
--potfile-disable	Ignore potfile and do not write
-d [#]	Specify an OpenCL Device
-D [#]	Specify an OpenCL Device type
-I	List OpenCL Devices & Types
-O	Optimized Kernel, Passwords <32 char
-i	Increment (brute force)
--increment-min [#]	Start increment at [#] of chars
--increment-max [#]	Stop increment at [#[of chars

hashcat-utils

Cap2hccapx (.pcap to WPA/WPA2)
./cap2hccapx.bin input.pcap output.hccapx [essid]

ct3_to_ntlm (mschap to ntlm)
./ct3_to_ntlm.bin 8-byte-ct3-in-hex 8-byte-salt-in-hex [24bESS]

deskey_2_ntlm (DES KPA to NTLM)
./deskey_to_ntlm.pl 8-byte-key-in-hex

keyspace (calculate keyspace with hashcat masks)
./keyspace.bin [options] mask

Keyspace Exhaustion At 229 GH/s

20 x ?a	2.2 T Solar orbits around the center of the Milky way*
10 x ?a	8,290 years
7 x ?a	3.4 days
5 x ?a	38 seconds
10 x ?l	7 days
7 x ?l	35 seconds
5 x ?l	51 milliseconds

*A solar orbit or "Cosmic Year" is the Sun orbiting the center of the Milkyway one time and takes approximately 225 million Earth years. Brute forcing a 20-character password with a 95 character mask at 229,000,000,000 hashes per second will take approximately 2.2 Trillion Cosmic Years.
95^20/229000000000/3600/24/365/255000000000~3,202,000,000,000 Years

USE WORDLISTS/DICTIONARIES

Common Dictionary Repos

CrackStation: https://crackstation.net/
Lots of others: https://wiki.skullsecurity.org/Passwords
Custom: cewl -d3 -w wordlist.txt -v http://domain.tld

Hash Sources to Hash Type

Inveigh NetNTLMv1	5500
Inveigh NetNTLMv2	5600
Mimikatz/LSAdump	1000
esedbexport/secretsdump.py ntds.dit (LM)	3000
esdbexport/secretsdump.py ntds.dit (NTLM)	1000
airmon-ng (WPA/WPA2)	2500
	2501

Common Hash Types

MD4	90
MD5	0
NTLM	1000
NetNTLMv1	5500
NetNTLMv2	5600
mscache1 (xp, w2k3)	1100
mscache2 (v, w7, w8, w10,w2k8+)	2100
LanManager	3000
SHA512	1700
Kerberos REQ	7500
Kerberos TGS-REP	13100
Wordpress	400
WPA	2500
WPA PMK	2501

Lookup Hash Modes (Type) from Command Line

```
hashcat --help| grep -I [keyword]
hashcat --help| grep -i salt
hashcat --help| grep -i Network
hashcat --help| grep -i raw
hashcat --help| grep -i Office
hashcat --help| grep -i Cisco
hashcat --help| grep -i Forum
hashcat --help| grep -i Domain
hashcat --help| grep -i SHA256
hashcat --help| grep -i MD5
```

Empty Hashes

LanManager aad3b435b51404eeaad3b435b51404ee
NTLM 31d6cfe0d16ae931b73c59d7e0c089c0

Lookup Hash Examples from Command Line

hashcat –example-hashes -m [hash-mode#]
NTLM – hashcat –example-hashes -m 1000

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

hashcat -b -m 900
Benchmark MD4 hashes

hashcat -m 13100 -a 0 --session crackin1 hashes.txt wordlist.txt -o output.pot
Create a hashcat session to hash Kerberos 5 tickets using wordlist.txt

hashcat -m 0 -a 3 -i hashes.txt ?a?a?a?a?a?a?a -o output.txt
Crack MD5 hashes using all characters in 7 character passwords

hashcat -m 100 -a 6 hashes.txt wordlist.txt ?a?a -o output.txt
Crack SHA1 by using wordlist with two ?a characters after

hashcat -m 13600 -a 3 hashes.txt ?u?l?l?l?l?l?d?d?d?d! -o output.txt
Crack WinZip hash, mask for Eighth2018!, Summer2018!, Etcetc5050

hashcat -a 0 -m 400 example400.hash example.dict
Crack PHPAss using dictionary file example.dict

hashcat -a 0 -m 0 example0.hash example.dict -r rules/best64.rule
Crack MD5 hashes using dictionary example.dict and modify with rules in best64.rule

hashcat -a 3 -m 0 example0.hash ?a?a?a?a?a?a
Crack MD5 using brute force with 6 characters that match the ?a characterset (upper, lower, numbers, symbols)

hashcat -a 1 -m 0 example0.hash example.dict example.dict
Crack MD5 using combinator function combining two dictionaries.