Hashcat

Source: https://hashcat.net

Hashcat is the advanced password recovery utility and it can generate combinations of brute-force attack possibilities.

Syntax

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

1. Hashcat Options
2. Hashcat-utils
3. Maskprocessor
4. Statsprocessor
5. Kwprocessor

1.Hashcat Options

Options

Option	Description
-m or --hash-type	Hash-type
-a or --attack-mode	Attack-mode
-V or --version	Print version
-h or --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-timer	Sets seconds between status screen updates to X
--stdin-timeout-abort	Abort if there is no input from stdin for X seconds
--machine-readable	Display the status view in a machine-readable format
--keep-guessing	Keep guessing the hash after it has been cracked
--self-test-disable	Disable self-test functionality on startup
--loopback	Add new plains to induct directory
--markov-hcstat2	Specify hcstat2 file to use
--markov-disable	Disables markov-chains, emulates classic brute-force
--markov-classic	Enables classic markov-chains
-t or --markov-threshold	Threshold X when to stop accepting new markov-chains
--runtime	Abort session after X seconds of runtime
--session	Define specific session name

Options

Option	Description
--restore	Restore session from --session
--restore-disable	Disable restored file
--restore-file-path	Specific path to restore file
-o or --outfile	Define outfile for recovered hash
--outfile-format	Define outfile-format X for recovered hash
--outfile-autohex-disable	Disable the use of $HEX[] in output plains
--outfile-check-timer	Sets seconds between outfile checks to X
--wordlist-autohex-disable	Disable the conversion of $HEX[] from the wordlist
-p or --separator	Separator char for hashlists and outfile
--stdout	Do not crack a hash, instead print candidates only
--show	Compare hashlist with potfile; show cracked hashes
--left	Compare hashlist with potfile; show uncracked hashes
--username	Enable ignoring of usernames in hashfile
--remove	Enable removal of hashes once they are cracked
--remove-timer	Enable removal of hashes once they are cracked
--potfile-disable	Do not write potfile
--encoding-from	Force internal wordlist encoding from X
--encoding-to	Force internal wordlist encoding to X
--debug-mode	Defines the debug mode
--debug-file	Output file for debugging rules
--induction-dir	Specify the induction directory to use for loopback
--logfile-disable	Disable the logfile
--hccapx-message-pair	Load only message pairs from hccapx matching X
--nonce-error-corrections	The BF size range to replace AP's nonce last byte
--keyboard-layout-mapping	Keyboard layout mapping table for special hash-modes
--truecrypt-keyfiles	Keyfiles to use, separated with commas
--veracrypt-keyfiles	VeraCrypt personal iterations multiplier

4. Mimikatz Kerberos Module

Options

Option	Description
-b or --benchmark	Run benchmark of selected hash-modes
--benchmark-all	Run benchmark of all hash-modes
--speed-only	Return expected speed of the attack, then quit
--progress-only	Return ideal progress step size and time to process
-c or --segment-size	Sets size in MB to cache from the word file to X
--bitmap-min	Sets minimum bits allowed for bitmaps to X
--bitmap-max	Sets maximum bits allowed for bitmaps to X
--cpu-affinity	Locks to CPU devices, separated with commas
--example-hashes	Show an example hash for each hash-mode
-I or --opencl-info	Show info about detected OpenCL platforms/devicess
--opencl-platforms	OpenCL platforms to use, separated with commas
-d or --opencl-devices	OpenCL devices to use, separated with commas
-D or --opencl-device-types	OpenCL device-types to use, separated with commas
--opencl-vector-width	Manually override OpenCL vector-width to X
-O or --optimized-kernel-enable	Enable optimized kernels (limits password length)
-w, --workload-profile	Enable a specific workload profile, see pool below
-n or --kernel-accel	Manual workload tuning, set outerloop step size to X
-u or --kernel-loops	Manual workload tuning, set innerloop step size to X
-T or --kernel-threads	Manual workload tuning, set thread count to X
--spin-damp	Use CPU for device synchronization, in percent
--hwmon-disable	Disable temperature and fanspeed reads and triggers
--hwmon-temp-abort	Abort if temperature reaches X degrees Celsius
--scrypt-tmto	Manually override TMTO value for scrypt to X
-s or --skip	Skip X words from the start

Options

Options	
`-1` or `--limit`	Limit X words from the start + skipped wordss
`--keyspace`	Show keyspace base:mod values and quit
`-j` `pr` `--rule-left`	Single rule applied to each word from left wordlist
`-k` or `--rule-right`	Single rule applied to each word from right wordlist
`-r` or `--rules-file`	Multiple rules applied to each word from wordlists
`-g` or `--generate-rules`	Generate X random rules
`--generate-rules-func-min`	Force max X functions per rule
`--generate-rules-func-max`	Force RNG seed set to X
`-1` or `--custom-charset1`	User-defined charset 1
`-2` or `--custom-charset2`	User-defined charset 2
`-3` or `--custom-charset3`	User-defined charset 3
`-4` or `--custom-charset4`	User-defined charset 4
`-i` or `-- --increment`	Enable mask increment mode
`--increment-min`	Start mask incrementing at X
`--increment-max`	Stop mask incrementing at X
`-S` or `--slow-candidates`	Enable slower (but advanced) candidate generators
`--brain-server`	Enable brain server
`--brain-client`	Abort session after X seconds of runtime
`--brain-client-features`	Define specific session name
`--brain-host`	Define specific session name
`--brain-port`	Define specific session name
`--brain-password`	Define specific session name
`--brain-session`	Define specific session name
`--brain-session-whitelist`	Define specific session name

2. Hashcat-utils

Utilities	Description
`cap2hccapx` Syntax: `./cap2hccapx.bin input.pcap output.hccapx [filter by essid] [additional network essid:bssid]`	Specifies a network name (ESSID) to filter out unwanted networks
`cleanup-rules` Syntax: `./cleanup-rules.bin mode`	Strips rules from STDIN that are not compatible with required platform
`combinator` Syntax: `./combinator.bin file1 file2`	Each word from file2 is appended to each word from file1 which is then printed to STDOUT
`combinator3`	Accepts three files as input, that produces the output combining all three lists
`combipow`	Produces all unique combinations from a shortlist of inputs
`cutb` Syntax: `./cutb.bin offset [length] < infile > outfile`	It will cut the specific prefix or suffix length off the existing words in a list and pass it to STDOUT
`expander`	Each word going into STDIN is parsed and split into all its single chars then sent to STDOUT
`gate` Syntax: `./gate.bin mod offset < infile > outfile`	Each wordlist going into STDIN is parsed split into equal sections and passed to STDOUT
`generate-rules` Syntax: `./generate-rules.bin number [seed]`	Stand-alone utility to generate random rules
`hcstatgen` Syntax: usage: `./hcstatgen.bin out.hcstat < infile`	Generates .hcstat files for use with older hashcats lcu
`hcstat2gen` Syntax: usage: `./hcstat2gen.bin outfile < dictionary`	Generates custom Markov statistics for use with hashcat's --markov-hcstat parameter
`keyspace` Syntax: `./keyspace.bin [options] mask`	Calculates keyspace in a hashcat-aware manner
`len` Syntax: `./len.bin min max < infile > outfile`	Each word going into STDIN is parsed for its length and passed to STDOUT if it matches a specified word-length range
`mli2` Syntax: `./mli2.bin infile mergefile`	Merges two lists
`morph` Syntax: `./morph.bin dictionary depth width pos_min pos_max`	Generates insertion rules for the most frequent chains of characters
`permute`	Each word going into STDIN is parsed and run through "The Countdown QuickPerm Algorithm"
`prepare`	Made as dictionary optimizer for Permutation attack
`req-include`	Each word going into STDIN is parsed and passed to STDOUT if it matches a specified password group criterion
`req-exclude`	Excludes words that match specific criteria
`rli` Syntax: usage: `rli infile outfile removefiles...`	Compares a single file against another file removing all duplicates
`splitlen` Syntax: `./splitlen.bin outdir < infile`	It is designed to be a dictionary optimizer for the now deprecated oclHashcat
`strip-bsn`	Strips all \0 bytes from stdin

Utilities	Description
`strip-bsr`	Strips all \r bytes from stdin
`tmesis`	Take wordlist and produce insertion rules
`tmesis-dynamic` Syntax: `./tmesis-dynamic.pl substring wordlist1.txt wordlist2.txt`	Take 2 wordlists and produces new one, using a user-defined substring as a "key"

3. Maskprocessor

Syntax

`./mp64.bin [options]... mask`

Options

Options	
`-V` or `--version`	Print version
`-h` or `--help`	Print help
`-I` or `--increment=NUM:NUM`	Enable increment mode. 1st NUM=start, 2nd NUM=stop
`--combinations`	Calculate number of combinations
`--hex-charset`	Assume charset is given in hex
`-q` or `--seq-max=NUM`	Maximum number of multiple sequential characters
`-r` or `--occurrence-max=NUM`	Maximum number of occurrences of a character
`-s` or `--start-at=WORD`	Start at specific position
`-l` or `--stop-at=WORD`	Stop at specific position
`-o` or `-output-file=FILE`	Output-file

4. Statsprocessor

Syntax

`./sp64.bin [options]... hcstat-file [filter-mask]`

Options

Options	
`-V` or `--version`	Print version
`-h` or `--help`	Print help
`--pw-min=NUM`	Start incrementing at NUM

4. Statsprocessor

Options	
--markov-disable	Emulates maskprocessor output
--markov-classic	No per-position tables
--threshold=NUM	Filter out chars after NUM chars added set to 0 to disable
--combinations	Calculate number of combinations
--hex-charset	Assume charset is given in hex
-s or --skip=NUM	Skip number of words (for restore)
-l or --limit=NUM	limit number of words (for distributed)
-o or --output-file=FILE	Output-file

2. Hashcat-utils

Syntax
./kwp [options]... basechars-file keymap-file routes-file

Options	
-V or --version	Print version
-h or --help	Print help
-o or --output-file	Output file
-b or --keyboard-basic	Include characters reachable without holding shift or altgr
-s or --keyboard-shift	Include characters reachable by holding shift
-a or --keyboard-altgr	Include characters reachable by holding altgr
-z or --keyboard-all	Shortcut to enable all --keyboard-* modifier
-1 or --keywalk-south-west	Include routes heading diagonal south-west
-2 or --keywalk-south	Include routes heading straight south
-3 or --keywalk-south-east	Include routes heading diagonal south-east
-4 or --keywalk-west	Include routes heading straight west

Options	
-5 or --keywalk-repeat	Include routes repeating character
-6 or --keywalk-east	Include routes heading straight east
-7 or --keywalk-north-west	Include routes heading diagonal north-west
-8 or --keywalk-north	Include routes heading straight north
-9 or --keywalk-north-east	Include routes heading diagonal north-east
-0 or --keywalk-all	Shortcut to enable all --keywalk-* directions
-n or --keywalk-distance-min	Minimum allowed distance between keys
-x or --keywalk-distance-max	Maximum allowed distance between keys