

Forum: [Hack Forums](#)

Thread: [\(Tutorial \) Cracking hashes with Hashcat with results](#)

Chorozon - March 2, 2025, 7:48 am

I have seen a bunch of half done "cracking" guides that basically quote documentation back to us leaving a thread full of confused commenters
today we are actually going to learn how to crack some hashes with hashcat
I know thats alot of hash and crack but we are going to get through it

First, grab a hash you want to crack. I am sure you have acquired them in a perfectly legal responsible education fashion

```
MD5 : 5f4dcc3bfed8b9c0b5d43e3a039d2e1a
NTLM : 8846fab98ef5bbd9a1d9f90b5d26fd56
SHA-1 : 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8
```

First, confirm Hashcat is installed (Kali has it by default):

Code hashcat --versionIf it responds with a version number (e.g., Hashcat (v7.00)), you're good to go.

Next, figure out your hash type . Run:

Code hashcat --helpSearch for your hash (e.g., 0 = raw MD5, 1000 = NTLM). Save your hash to a file, like hashes.txt.

Now we are all set up and know our hash type

Let's start with a basic dictionary attack. Kali has preloaded wordlists in /usr/share/wordlists/:

Code hashcat -m [hash_type] hashes.txt /usr/share/wordlists/rockyou.txtExample for an NTLM hash:

Code hashcat -m 1000 hashes.txt /usr/share/wordlists/rockyou.txtThis tries 14 million common passwords. If you see [FOUND] in the output, congrats!

? This is what all the other guides won't cover

What do you do if Cracking Isn't Working...

[/b]

1. Try a Bigger Wordlist

Kali's rockyou.txt is great, but some passwords are trickier. Grab lists from:

GitHub's SecLists : git clone <https://github.com/danielmiessler/SecLists>

Custom lists : Use cewl to generate lists from target websites:

Code `cewl -w custom.txt https://target-website.com`

2. Add Rules

Rules tweak dictionary words (e.g., uppercase, add numbers). Example:

Code `hashcat -m 1000 hashes.txt /usr/share/wordlists/rockyou.txt -r /usr/share/hashcat/rules/best64.rule` This tries Password, pASSWORD, Password1, etc.

3. Brute-Force with Masks

For passwords with patterns (e.g., Passw0rd), use masks:

Code `hashcat -m 0 hashes.txt ?l?l?l?d?d?d -o cracked.txt`

?l = lowercase, ?d = digits

This guesses 3-letter + 3-digit combos (e.g., cat123).

4. Speed It Up with GPUs

Hashcat uses your GPU by default this is one of the reasons your cracking is not successful . Make sure to check performance with:

Code `hashcat -b` Install OpenCL drivers if missing (Kali usually has them but shit happens).

Combine wordlists and masks:

Code `hashcat -m 1000 hashes.txt -a 0 -1 ?l?d rockyou.txt ?1?1?1?1`

Hybrid attacks (dictionary + masks):

Code `hashcat -m 1000 hashes.txt -a 6 -1 ?l?d rockyou.txt ?1`

? Great Success!

Cracked passwords appear in cracked.txt (or your specified output file). If nothing works, try:

Updating Hashcat (`sudo apt update && sudo apt install hashcat`).

Mixing rules and masks.

Upgrading hardware (GPUs crush hashes faster. your shitty rdp/vm might not be up to it).

HOT TIP : COLLECT PASSWORD BREACHS / LISTS IN MULTIPLE LANGUAGES

Pr0m3th3us - March 2, 2025, 7:47 pm

Nice TUT as usual, thank you