# Crackin' Hashes with



advanced password recovery

# Hashcat usage

Syntax

hashcat -a <attack mode> -m <hash type> <file to crack> <wordlist>

-a <attack mode>

- There are 6 different modes of attack, we'll discuss the four most common ones
- 0 | Straight
- 1 | Combination
- 3 | Brute-force
- 6 | Hybrid Wordlist + Mask
- 7 | Hybrid Mask + Wordlist
- 9 | Association

-m <hash type>

• There are waaaaaay too many hash types to list here, but you can see them all by entering the command hashcat --help

<file to crack>

• This will be the file which contains the hash.

<wordlist>

• This will be the list of words used to crack the hash

CRC32

MD5

SHA-256

Doctor's prescription note

The property of th



1.hash – Dictionary Attack

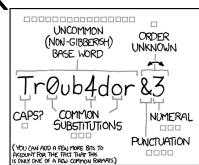
- Mode
  - -a 0

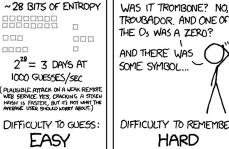
Cracking passwords is, unfortunately, very easy to do. It just takes hardware and time.

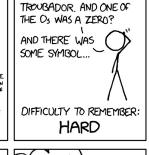
 First, we'll need to identify the hash. hashid 1.hash -m

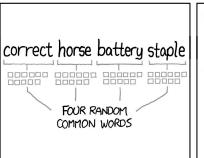
Then we can crack the hash.

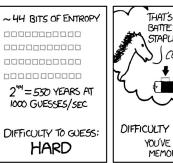
hashcat -a 0 -m <hash type> 1.hash passwordlist.txt

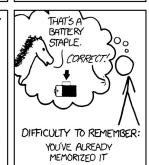












THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

## 2.hash – Dictionary Attack

- Mode
  - -a 0
- First, we'll need to identify the hash.

hashid 2.hash –m

• Then we can crack the hash.

hashcat -a 0 -m <hash type> 2.hash passwordlist.txt





### 3.hash - Combination Attack

- Mode
  - -a 1
- First, we'll need to identify the hash.

```
hashid 3.hash -m
```

 For this one, we're going to use two separate password lists to crack the hash.

hashcat -a 1 -m <hash type> 3.hash passwordlist.txt passwordlist2.txt



**YOUR LAST NAME** 

c-c-c-COMBO!

#### 4.hash – Mask Mode

- Mode
  - -a3
- First, we'll need to identify the hash.

hashid 4.hash –m

- If we have a good idea of what the password may be, or if we just want to try, we can use placeholders.
  - ?l: Lower-case ASCII letters (a-z)
  - ?u: Upper-case ASCII letters (A-Z)
  - ?d: Digits (0-9)
  - ?h: Lower-case hexadecimal characters (0123456789abcdef)
  - ?H: Upper-case hexadecimal characters (0123456789ABCDEF)
  - ?s: Special characters (space, !"#\$%&'()\*+,-./:;<=>?@[]^\_`{|}~)
  - ?a: All printable ASCII characters (combination of ?l, ?u, ?d, and ?s)
  - ?b: All possible byte values (0x00 0xff)
- Now we can crack the hash

hashcat -a 3 -m <hash type> 4.hash -1 01 'Lenovo?d?d?d?d?s'



## 5.hash – Hybrid Mode

- Mode
  - -a 6
- First, we'll need to identify the hash.
   hashid 5.hash -m
- We can also use placeholders in conjunction with wordlists.

You successfully launched a dictionary attack for your cyber security course and cracked the password.

The cracked password is your password.



Now we can crack the hash.

hashcat -a 6 -m <hash type> 5.hash passwordlist.txt '?d?d?d?d'