
ATTACK
DEFENSE
by PentesterAcademy

Name	Cracking MD5 Hashes
URL	https://www.attackdefense.com/challengedetails?cid=51
Type	Cracking : Hashcat All

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic.

User should try dictionary attack using the provided dictionary file first. If the dictionary attack doesn't succeeds, then the user should go for mask based bruteforce approach according to given password policy.

Step 1: Check the given MD5 hash.

```
student@attackdefense:~$ cat digest.txt
813446902666d346ab42151a3beaf5a9
student@attackdefense:~$
```

Step 2: Try dictionary attack using given dictionary file 1000000-password-seclists.txt

Command: hashcat -m 0 -a 0 digest.txt 1000000-password-seclists.txt

Explanation

-m 0 : MD5 hash mode
-a 0 : Dictionary attack mode

The attack won't succeed. Hence, we will move to mask based attack.

As per given password policy, the length of the password is less than 6 characters and it is made up of this character set: a-z, 0-9

Step 3: Launch the mask based attack.

Command: hashcat -m 0 digest.txt -a 3 -1 ?l?d ?1?1?1?1?1

Explanation

-m 0	:	MD5 hash mode
-a 3	:	Mask mode
-1 ?l?d ?1?1?1?1?1	:	l (small L) signifies group (a-z) and d (minor D) signifies group (0-9)

```
813446902666d346ab42151a3beaf5a9:1a23b

Session..........: hashcat
Status...........: Cracked
Hash.Type........: MD5
Hash.Target......: 813446902666d346ab42151a3beaf5a9
Time.Started.....: Sat Nov  3 21:35:18 2018 (2 secs)
Time.Estimated...: Sat Nov  3 21:35:20 2018 (0 secs)
Guess.Mask.......: ?1?1?1?1?1 [5]
Guess.Charset....: -1 ?l?d, -2 Undefined, -3 Undefined, -4 Undefined
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#1.....: 13713.3 kH/s (47.73ms) @ Accel:1024 Loops:36 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 28753920/60466176 (47.55%)
Rejected.........: 0/28753920 (0.00%)
Restore.Point....: 778240/1679616 (46.33%)
Candidates.#1....: skt0r -> xcicb
HWMon.Dev.#1.....: N/A

Started: Sat Nov  3 21:35:09 2018
Stopped: Sat Nov  3 21:35:21 2018
```

Flag: 1a23b

References:

1. Hashcat (https://hashcat.net)
2. Hashcat Wiki (https://hashcat.net/wiki/)