
ATTACK
DEFENSE
by PentesterAcademy

Name	Cracking MD5Crypt Digests
URL	https://www.attackdefense.com/challengedetails?cid=60
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: An MD5Crypt digest is provided in digest.txt file. Check the file contents.

```
student@attackdefense:~$ cat digest.txt
$1$s1ty35f$Si..C51.0l58LJ76G7crB/
student@attackdefense:~$
```

Step 1: Try the dictionary attack using given dictionary file 1000000-password-seclists.txt

Command: hashcat -m 500 digest.txt -a 0 1000000-password-seclists.txt

Explanation

-m 500 : MD5Crypt digest mode
-a 0 : Dictionary attack mode

```
$1$s1ty35f$Si..C51.0l58LJ76G7crB/:zombizombi

Session..........: hashcat
Status...........: Cracked
Hash.Type........: md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5)
Hash.Target......: $1$s1ty35f$Si..C51.0l58LJ76G7crB/
Time.Started.....: Sun Nov  4 01:22:21 2018 (1 min, 57 secs)
Time.Estimated...: Sun Nov  4 01:24:18 2018 (0 secs)
Guess.Base.......: File (1000000-password-seclists.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#1.....:     3219 H/s (181.63ms) @ Accel:512 Loops:62 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 378880/1000003 (37.89%)
Rejected.........: 0/378880 (0.00%)
Restore.Point....: 368640/1000003 (36.86%)
Candidates.#1....: 020789n -> Wonder12
HWMon.Dev.#1.....: N/A
```

Flag: zombizombi

References:

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