
ATTACK
DEFENSE
by PentesterAcademy

Name	Cracking SHA-3 Digests
URL	https://www.attackdefense.com/challengedetails?cid=57
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 file contents.

```
student@attackdefense:~$ cat digest.txt
0aa8ffe277db824c20eb5d0cb3ea78cb6ab74093249cae3c762f2b7d1c56c881
student@attackdefense:~$
```

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

Command: hashcat -m 5000 digest.txt -a 0 1000000-password-seclists.txt

Explanation

-m 5000 : SHA-3 digest mode
-a 0 : Dictionary attack mode

The attack will succeed.

```
0aa8ffe277db824c20eb5d0cb3ea78cb6ab74093249cae3c762f2b7d1c56c881:vjhtrhsvdctcegth

Session..........: hashcat
Status...........: Cracked
Hash.Type........: SHA-3 (Keccak)
Hash.Target......: 0aa8ffe277db824c20eb5d0cb3ea78cb6ab74093249cae3c762...56c881
Time.Started.....: Sun Nov  4 01:09:05 2018 (2 secs)
Time.Estimated...: Sun Nov  4 01:09:07 2018 (0 secs)
Guess.Base.......: File (1000000-password-seclists.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#1.....:   716.8 kH/s (20.68ms) @ Accel:1024 Loops:1 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 1000003/1000003 (100.00%)
Rejected.........: 9/1000003 (0.00%)
Restore.Point....: 983049/1000003 (98.30%)
Candidates.#1....: vrs000 -> vjht008
HWMon.Dev.#1.....: N/A
```

Flag: vjhtrhsvdctcegth

References:

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