ATTACK DEFENSE

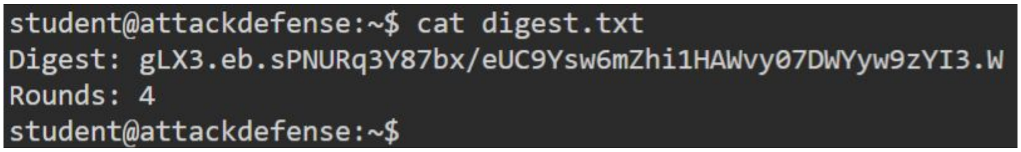
by PentesterAcademy

Name	Cracking Bcrypt Hashes
URL	https://www.attackdefense.com/challengedetails?cid=61
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.

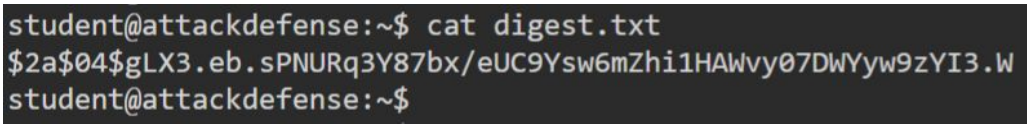
User should try dictionary attack using the provided dictionary file first. If the dictionary attack doesn't succeeds, then the user should go for mask based bruteforce approach according to given password policy.

Step 1: Bcrypt hash in digest.txt file. Check the digest file.



```
student@attackdefense:~$ cat digest.txt
Digest: gLX3.eb.sPNURq3Y87bx/eUC9Ysw6mZhi1HAWvy07DWYyw9zYI3.W
Rounds: 4
student@attackdefense:~$
```

This input format is not compatible to Hashcat. So, modify it.



```
student@attackdefense:~$ cat digest.txt
$2a$04$gLX3.eb.sPNURq3Y87bx/eUC9Ysw6mZhi1HAWvy07DWYyw9zYI3.W
student@attackdefense:~$
```

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

Command: hashcat -m 3200 -a 0 digest.txt 1000000-password-seclists.txt

Explanation

-m 1000 : Bcrypt hash mode

-a 0 : Dictionary attack mode

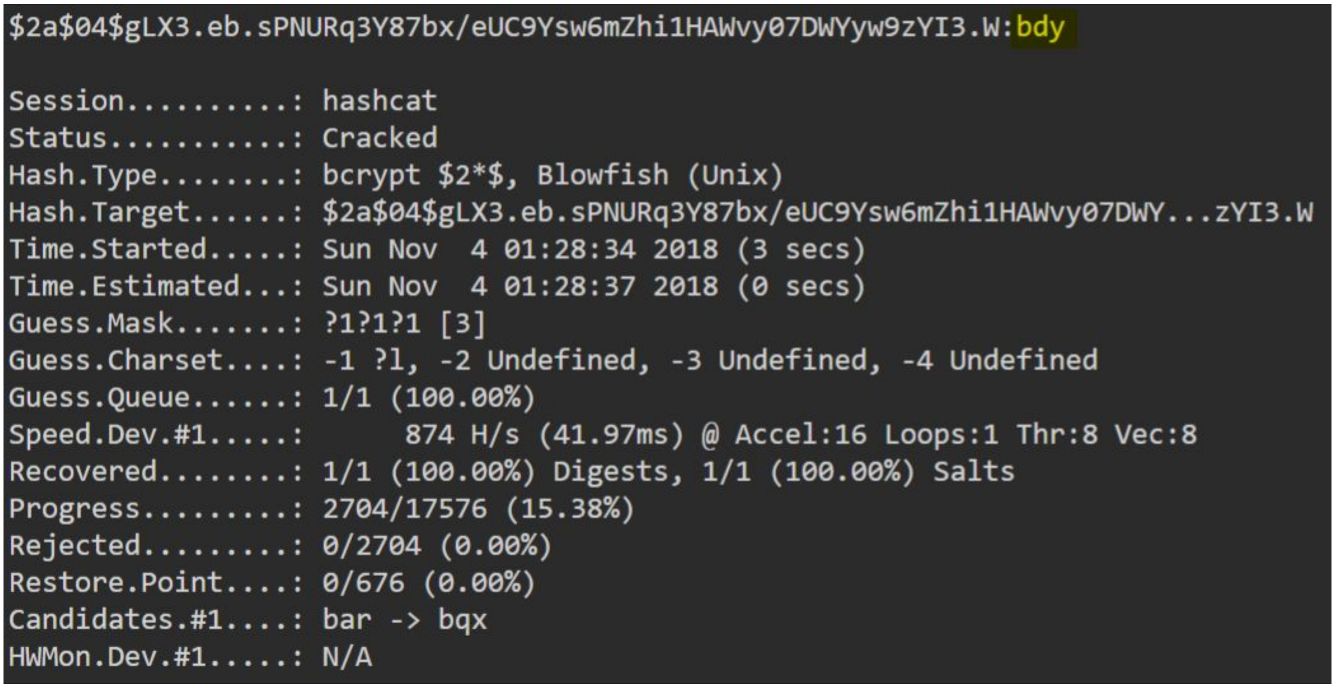
Step 3: Attack won't succeed. So, move to mask based attack.

As per given password policy, the length of the password is less than 4 characters and it is made up of this character set: a-z, 0-9

Command: hashcat -m 3200 digest.txt -a 3 -1 ?l?d ?1?1?1

Explanation

-m 3200 : Bcrypt hash mode
-a 3 : Mask mode
-1 ?l?d ?1?1?1 : l (small L) signifies group (a-z) and d (minor D) signifies group (0-9)



```
$2a$04$gLX3.eb.sPNURq3Y87bx/eUC9Ysw6mZhi1HAWvy07DWYyw9zYI3.W:bdy

Session..........: hashcat
Status...........: Cracked
Hash.Type........: bcrypt $2*$, Blowfish (Unix)
Hash.Target......: $2a$04$gLX3.eb.sPNURq3Y87bx/eUC9Ysw6mZhi1HAWvy07DWY...zYI3.W
Time.Started.....: Sun Nov  4 01:28:34 2018 (3 secs)
Time.Estimated...: Sun Nov  4 01:28:37 2018 (0 secs)
Guess.Mask.......: ?1?1?1 [3]
Guess.Charset....: -1 ?l, -2 Undefined, -3 Undefined, -4 Undefined
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#1.....:      874 H/s (41.97ms) @ Accel:16 Loops:1 Thr:8 Vec:8
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 2704/17576 (15.38%)
Rejected.........: 0/2704 (0.00%)
Restore.Point....: 0/676 (0.00%)
Candidates.#1....: bar -> bqx
HWMon.Dev.#1.....: N/A
```

Flag: bdy

References:

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