
ATTACK
DEFENSE
by PentesterAcademy

Name	Cracking 7z Archives
URL	https://www.attackdefense.com/challengedetails?cid=94
Type	Cracking : Protected Files

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: A 7zip archive file is given. Extract the crackable information from the file using John the Ripper tools and check file contents

Command: 7z2john archive.7z > hash

```
student@attackdefense:~$ cat hash
archive.7z:$7z$2$19$0$$8$6b785510465f9d2b0000000000000000$751724903$48$37$8dcf833392a1b
a344c99b1fe93a1c83d1cd76c01$33$00
student@attackdefense:~$
```

Step 2: We can use either of two tools

John The Ripper (JTR)

Launch dictionary attack using given dictionary file 1000000-password-seclists.txt

Command: john --wordlist=1000000-password-seclists.txt hash

```
student@attackdefense:~$  john --wordlist=1000000-password-seclists.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 20 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
yankees          (archive.zip)
1g 0:00:00:00 DONE (2018-11-04 02:16) 100.0g/s 4096Kp/s 4096Kc/s 4096KC/s 123456..taint
Use the "--show" option to display all of the cracked passwords reliably
Session completed
student@attackdefense:~$
```

The attack won't succeed. So, move to mask based attack.

As per given password policy, the length of the password is less than 5 characters and it is made up of this character set: 0-9

Command: john --mask=?1?1?1?1 -1=?d -min-len=4 -max-len=4 hash

Explanation

--mask=?1?1?1?1	:	Define mask of length 4 characters
-1=?d	:	d (minor D) signifies group (0-9)
-min-len=4 -max-len=4	:	Min and max length of password

```
student@attackdefense:~$ john --mask=?1?1?1?1 -1=?d -min-len=4 -max-len=4 hash
Using default input encoding: UTF-8
Loaded 1 password hash (7z, 7-Zip [SHA256 256/256 AVX2 8x AES])
Cost 1 (iteration count) is 524288 for all loaded hashes
Cost 2 (padding size) is 11 for all loaded hashes
Cost 3 (compression type) is 2 for all loaded hashes
Will run 20 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
6132             (archive.7z)
1g 0:00:00:51 DONE (2018-11-04 02:36) 0.01942g/s 46.62p/s 46.62c/s 46.62C/s 1922..7732
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Flag: 6132

Hashcat (JTR)

Make extracted crackable information hashcat compatible.

```
student@attackdefense:~$ cat hash
$7z$2$19$0$$8$6b785510465f9d2b0000000000000000$751724903$48$37$8dcf833392a1b06fe840ea74
93a1c83d1cd76c01$33$00
student@attackdefense:~$
```

Launch mask based attack on the extracted information.

Command: hashcat -m 11600 hash -a 3 -1 ?d ?1?1?1?1

Explanation

-m 11600	:	7z hash mode
-a 3	:	Mask mode
-1 ?d ?1?1?1?1	:	d (minor D) signifies group (0-9)

```
$7z$2$19$0$$8$6b785510465f9d2b0000000000000000$751724903$48$37$8dcf833392a1b06fe840ea74
93a1c83d1cd76c01$33$00:6132

Session..........: hashcat
Status...........: Cracked
Hash.Type........: 7-Zip
Hash.Target......: $7z$2$19$0$$8$6b785510465f9d2b0000000000000000$7517...$33$00
Time.Started.....: Sun Nov  4 02:38:55 2018 (17 mins, 51 secs)
Time.Estimated...: Sun Nov  4 02:56:46 2018 (0 secs)
Guess.Mask.......: ?1?1?1?1 [4]
Guess.Charset....: -1 ?d, -2 Undefined, -3 Undefined, -4 Undefined
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#1.....:        9 H/s (0.15ms) @ Accel:960 Loops:16 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 10000/10000 (100.00%)
Rejected.........: 0/10000 (0.00%)
Restore.Point....: 0/1000 (0.00%)
Candidates.#1....: 6234 -> 6764
HWMon.Dev.#1.....: N/A
```

Flag: 6132

References:

1. Hashcat (https://hashcat.net)
2. Hashcat Wiki (https://hashcat.net/wiki/)
3. John the ripper jumbo (https://www.openwall.com/john/)