ATTACK DEFENSE

by PentesterAcademy

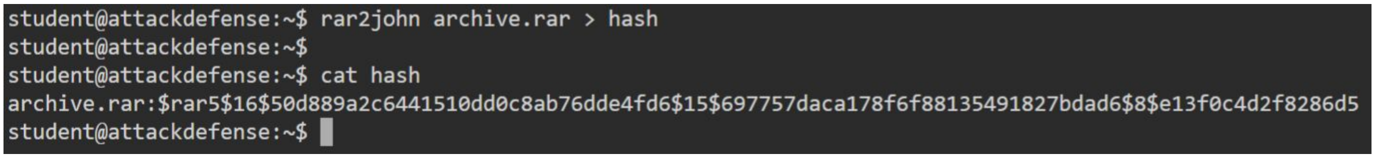
Name	Cracking RAR Archives
URL	https://www.attackdefense.com/challengedetails?cid=96
Type	Cracking : Protected Files

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 RAR archive file is given. Extract the crackable information from the file using John the Ripper tools and check file contents

Command: rar2john archive.rar > hash



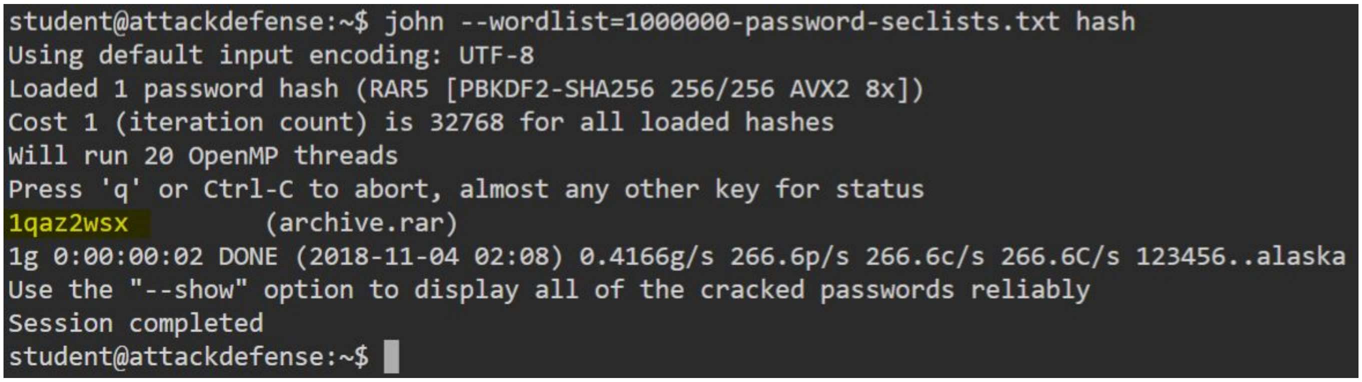
```
student@attackdefense:~$ rar2john archive.rar > hash
student@attackdefense:~$
student@attackdefense:~$ cat hash
archive.rar:$rar5$16$50d889a2c6441510dd0c8ab76dde4fd6$15$697757daca178f6f88135491827bdad6$8$e13f0c4d2f8286d5
student@attackdefense:~$ 
```

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



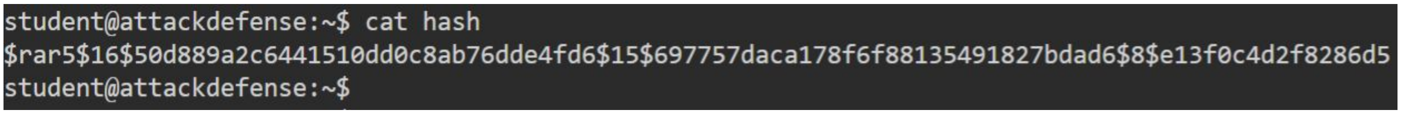
```
student@attackdefense:~$ john --wordlist=1000000-password-seclists.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (RAR5 [PBKDF2-SHA256 256/256 AVX2 8x])
Cost 1 (iteration count) is 32768 for all loaded hashes
Will run 20 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
1qaz2wsx         (archive.rar)
1g 0:00:00:02 DONE (2018-11-04 02:08) 0.4166g/s 266.6p/s 266.6c/s 266.6C/s 123456..alaska
Use the "--show" option to display all of the cracked passwords reliably
Session completed
student@attackdefense:~$ 
```

Flag: 1qaz2wsx

Hashcat (JTR)

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

Convert the extracted information to hashcat compatible format.

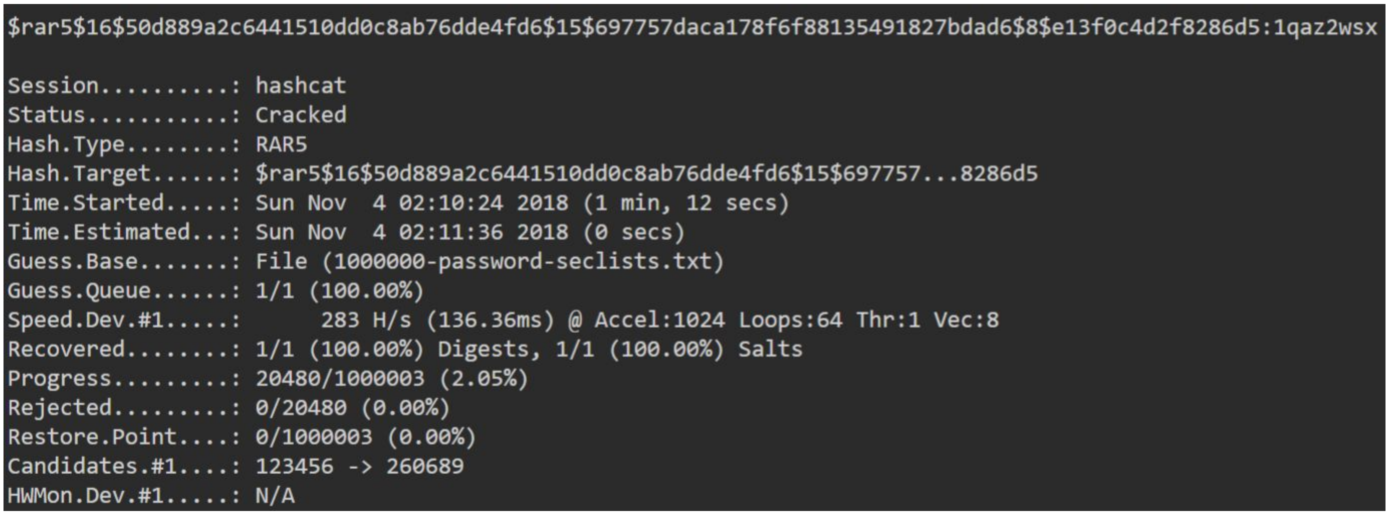


```
student@attackdefense:~$ cat hash
$rar5$16$50d889a2c6441510dd0c8ab76dde4fd6$15$697757daca178f6f88135491827bdad6$8$e13f0c4d2f8286d5
student@attackdefense:~$
```

Command: hashcat -m 13000 hash -a 0 1000000-password-seclists.txt

Explanation

-m 13000	:	RAR format
-a 0	:	Dictionary mode



```
$rar5$16$50d889a2c6441510dd0c8ab76dde4fd6$15$697757daca178f6f88135491827bdad6$8$e13f0c4d2f8286d5:1qaz2wsx

Session..........: hashcat
Status...........: Cracked
Hash.Type........: RAR5
Hash.Target......: $rar5$16$50d889a2c6441510dd0c8ab76dde4fd6$15$697757...8286d5
Time.Started.....: Sun Nov  4 02:10:24 2018 (1 min, 12 secs)
Time.Estimated...: Sun Nov  4 02:11:36 2018 (0 secs)
Guess.Base.......: File (1000000-password-seclists.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#1.....:      283 H/s (136.36ms) @ Accel:1024 Loops:64 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 20480/1000003 (2.05%)
Rejected.........: 0/20480 (0.00%)
Restore.Point....: 0/1000003 (0.00%)
Candidates.#1....: 123456 -> 260689
HWMon.Dev.#1.....: N/A
```

Flag: 1qaz2wsx

References:

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