
ATTACK
DEFENSE
by PentesterAcademy

Name	Cracking PKZIP Archives
URL	https://www.attackdefense.com/challengedetails?cid=95
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 ZIP archive file is given. Extract the crackable information from the file using John the Ripper tools and check file contents

Command: zip2john archive.zip > hash

```
student@attackdefense:~$ zip2john archive.zip > hash
ver 1.0 efh 5455 efh 7875 archive.zip->token PKZIP Encr: 2b chk, TS_chk, cmplen=45, dec
student@attackdefense:~$
student@attackdefense:~$ cat hash
archive.zip:$pkzip2$1*2*2*0*2d*21*c10509e*0*3f*0*2d*0c10*360a*f5e92c2b27b0f6ece97e6030c
410a770aa*$/pkzip2$:::::archive.zip
student@attackdefense:~$
```

Step 2: We have to use JTR because at the time of writing this document, PKZIP is not supported by hashcat.

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:~$
```

Flag: yankees

References:

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