# ATTACK DEFENSE

by PentesterAcademy

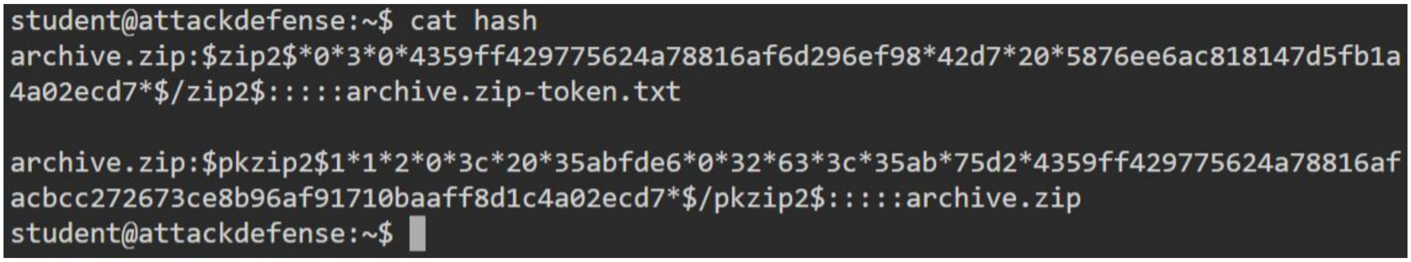
| | |
|---|---|
| **Name** | Cracking WinZip Archives |
| **URL** | https://www.attackdefense.com/challengedetails?cid=93 |
| **Type** | Cracking : Protected Files |

**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 winzip 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



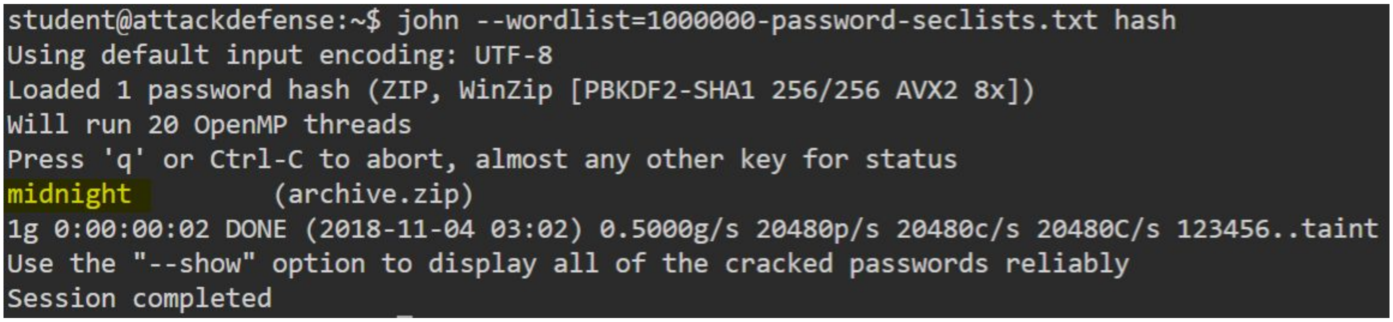
```
student@attackdefense:~$ cat hash
archive.zip:$zip2$*0*3*0*4359ff429775624a78816af6d296ef98*42d7*20*5876ee6ac818147d5fb1a
4a02ecd7*$/zip2$::::archive.zip-token.txt

archive.zip:$pkzip2$1*1*2*0*3c*20*35abfde6*0*32*63*3c*35ab*75d2*4359ff429775624a78816af
acbcc272673ce8b96af91710baaff8d1c4a02ecd7*$/pkzip2$::::archive.zip
student@attackdefense:~$ 
```

**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

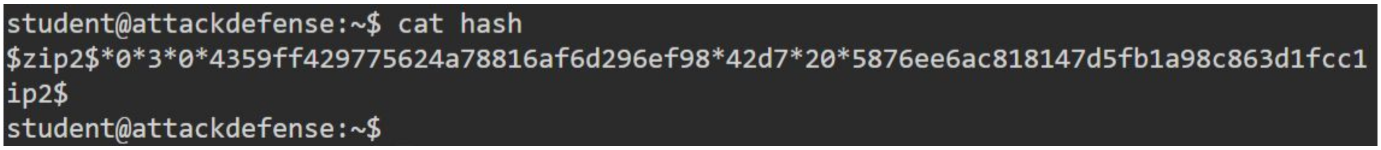


```
student@attackdefense:~$ john --wordlist=1000000-password-seclists.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Will run 20 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
midnight         (archive.zip)
1g 0:00:00:02 DONE (2018-11-04 03:02) 0.5000g/s 20480p/s 20480c/s 20480C/s 123456..taint
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

**Flag:** midnight

### Hashcat (JTR)

Make extracted crackable information hashcat compatible.

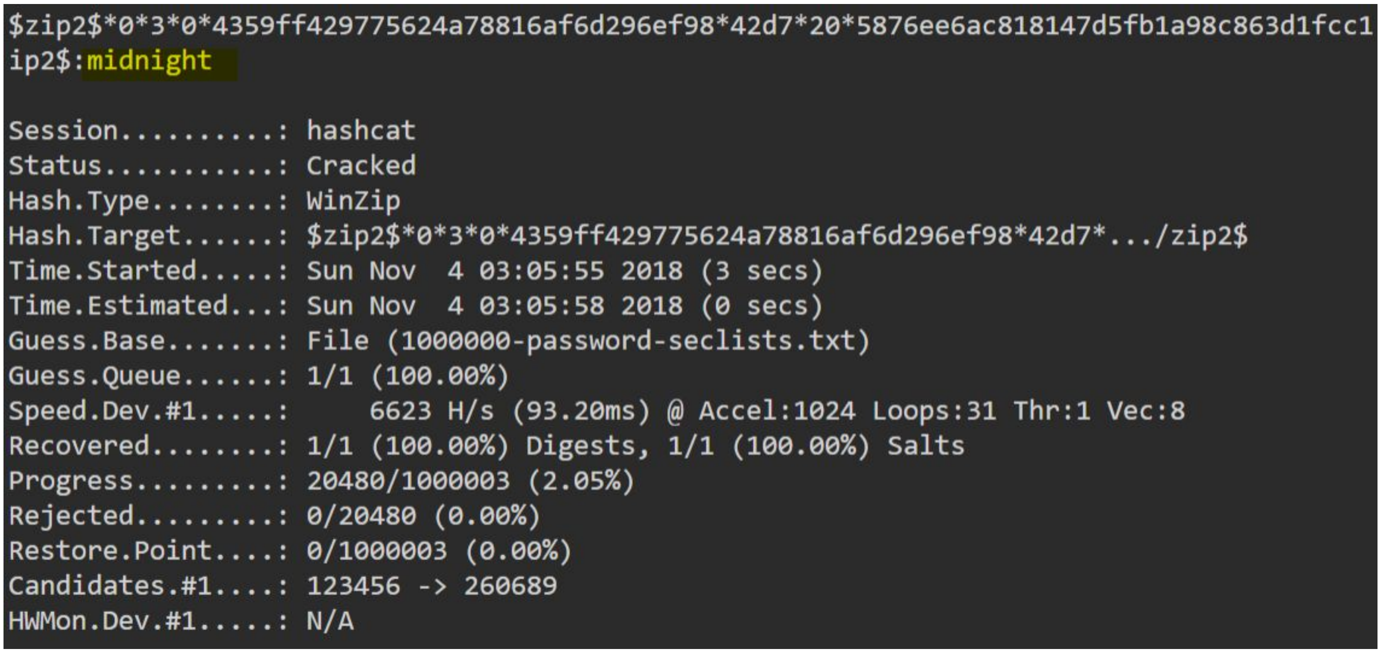


```
student@attackdefense:~$ cat hash
$zip2$*0*3*0*4359ff429775624a78816af6d296ef98*42d7*20*5876ee6ac818147d5fb1a98c863d1fcc1
ip2$
student@attackdefense:~$
```

**Command:** hashcat -m 13600 hash -a 0 1000000-password-seclists.txt

Explanation

| | | |
|---|---|---|
| -m 13600 | : | WinZip format |
| -a 0 | : | Dictionary mode |



```
$zip2$*0*3*0*4359ff429775624a78816af6d296ef98*42d7*20*5876ee6ac818147d5fb1a98c863d1fcc1
ip2$:midnight

Session..........: hashcat
Status...........: Cracked
Hash.Type........: WinZip
Hash.Target......: $zip2$*0*3*0*4359ff429775624a78816af6d296ef98*42d7*.../zip2$
Time.Started.....: Sun Nov  4 03:05:55 2018 (3 secs)
Time.Estimated...: Sun Nov  4 03:05:58 2018 (0 secs)
Guess.Base.......: File (1000000-password-seclists.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#1.....:     6623 H/s (93.20ms) @ Accel:1024 Loops:31 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:** midnight

**References:**

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