hashcat破解压缩包密码（7z/rar/zip)

> hashcat利用GPU进行破解速度会更快。

一、 7z格式压缩包破解

1. 生成hash文件

```
7z2john 7zdecrypt.txt.7z > 7z.hash
```

> 运行`7z2john`的时候可能会报错，显示缺少算法模块`lzma`。安装该模块即可。
>
> ```
> sudo apt install libcompress-raw-lzma-perl
> ```

2. 修改hash文件

打开文件`7z.hash`，去掉`hash`值之前的文件名称及冒号。（否则`hashcat`会报错，无法处理该内容。使用`john`破解时则无需修改）

- 修改前：

  ```
  7zdecrypt.txt.7z:$7z$2$19$0$$8$1628f11dfc0f2e32000000000000000$2940131417$48$46$47daba4f2222c6f58f3053e9a33942580bd388bd7915b4978ac59523adcbf52185bd4b9597ba5de3fd2dd45506502f5a$42$00
  ```

- 修改后

  ```
  $7z$2$19$0$$8$1628f11dfc0f2e32000000000000000$2940131417$48$46$47daba4f2222c6f58f3053e9a33942580bd388bd7915b4978ac59523adcbf52185bd4b9597ba5de3fd2dd45506502f5a$42$00
  ```

3. 使用hashcat破解

`7-Zip`对应的`hash`模式为`11600`。

```
hashcat -m 11600 7z.hash /usr/share/wordlists/rockyou.txt
```

4. 密码验证

对`7z`压缩包进行解压，验证密码是否正确。

```
7z e 7zdecrypt.txt.7z
```

二、rar格式压缩包破解

1. 生成hash文件

```
rar2john rardecrypt.txt.rar > rar.hash
```

2. 修改hash文件

打开文件`rar.hash`，去掉`hash`值之前的文件名称及冒号。

- 修改前：

  ```
  rardecrypt.txt.rar:$rar5$16$2e2b531a2840a77769e16d87514f591a$15$0e08594df8b48e305f98b070159d00dc$8$423c1a7a18816932
  ```

- 修改后

  ```
  $rar5$16$2e2b531a2840a77769e16d87514f591a$15$0e08594df8b48e305f98b070159d00dc$8$423c1a7a18816932
  ```

3. 使用hashcat破解

`RAR5`对应的`hash`模式为`13000`。

```
hashcat -m 13000 rar.hash /usr/share/wordlists/rockyou.txt
```

4. 密码验证

对`rar`压缩包进行解压，验证密码是否正确。

```
rar e rardecrypt.txt.rar
```

三、zip格式压缩包破解

1. 生成hash文件

```
zip2john zipdecrypt.txt.zip > zip.hash
```

2. 修改hash文件

打开文件`zip.hash`，去掉`hash`值前后的文件名称及冒号。

- 修改前：

```
zipdecrypt.txt.zip/zipdecrypt.txt:$pkzip$1*2*2*0*37*2b*887a34f6*0*48*0*37*b
859*4041d4c6cedacd9b29a3cc761c54129fad8d94c262bb36fae1770dff1b6627dbca65527
d39f22fbb8e4e32197f695a9bcc284b075dd310*$/pkzip$:zipdecrypt.txt:zipdecrypt.
txt.zip::zipdecrypt.txt.zip
```

- 修改后：

```
$pkzip$1*2*2*0*37*2b*887a34f6*0*48*0*37*b859*4041d4c6cedacd9b29a3cc761c5412
9fad8d94c262bb36fae1770dff1b6627dbca65527d39f22fbb8e4e32197f695a9bcc284b075
dd310*$/pkzip$
```

3. 使用hashcat破解

`PKZIP (Mixed Multi-File)`对应的`hash`模式为`17225`。

```
hashcat -m 17225 zip.hash /usr/share/wordlists/rockyou.txt
```

4. 密码验证

对`zip`压缩包进行解压，验证密码是否正确。

```
unzip zipdecrypt.txt.zip
```

附：

使用john破解压缩包：

- 7z

```
john --format=7z --wordlist=/usr/share/wordlists/rockyou.txt 7z.hash
```

- rar

```
john --format=RAR5 --wordlist=/usr/share/wordlists/rockyou.txt rar.hash
```

- zip

```
john --format=PKZIP --wordlist=/usr/share/wordlists/rockyou.txt zip.hash
```