

# 破解压缩文件密码

## 实验环境

Kali

## 实验步骤

### 创建文件

```
(root@kali)-[~]
# touch {1..3}.txt

(root@kali)-[~]
# ls
1.txt 2.txt 3.txt Desktop Documents Downloads Music Pictures Public Templates test.txt Videos

(root@kali)-[~]
# rar a test 1.txt 2.txt 3.txt -p 创建rar类型的压缩包

Enter password (will not be echoed):123456

Reenter password:123456

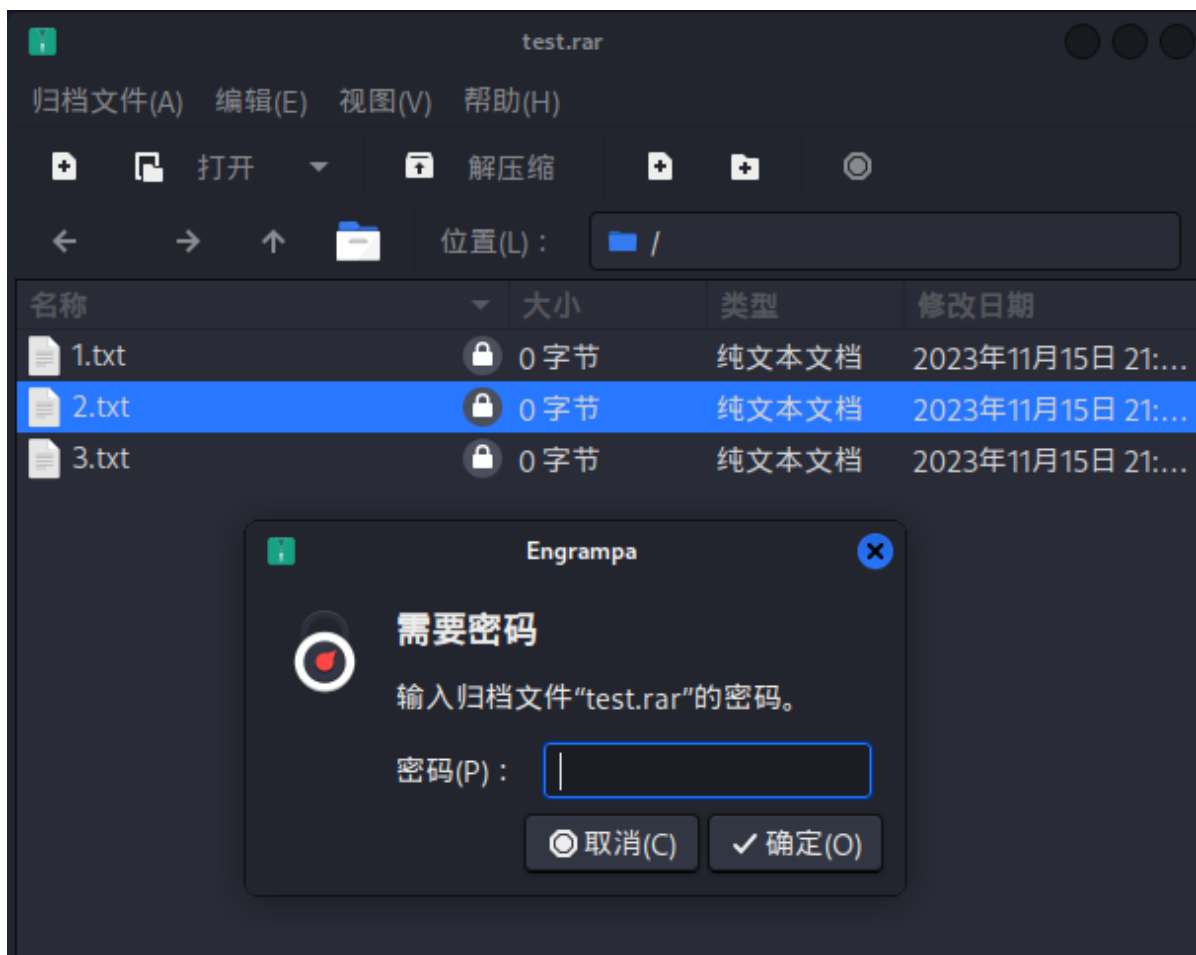
RAR 6.23 Copyright (c) 1993-2023 Alexander Roshal 1 Aug 2023
Trial version Type 'rar -?' for help

Evaluation copy. Please register.

Creating archive test.rar

Adding 1.txt OK
Adding 2.txt OK
Adding 3.txt OK
Done

(root@kali)-[~]
# ls
1.txt 3.txt Documents Music Public test.rar Videos
2.txt Desktop Downloads Pictures Templates test.txt
```



## 使用字典破解密码

```
(root@kali)-[~]
# rar2john test.rar
Created directory: /root/.john
test.rar:$rar5$16$96e04fc35f40d9aceb1de854d4d07bf0$15$cc3fa14f46076277ae4040702d8fa872$8$8f12b9653222a7d8
test.rar:$rar5$16$96e04fc35f40d9aceb1de854d4d07bf0$15$cc40768ad3171a7933451a72abe1f86b$8$8f12b9653222a7d8
test.rar:$rar5$16$96e04fc35f40d9aceb1de854d4d07bf0$15$7842becbabe542d6dc162c0973e2a3a8$8$8f12b9653222a7d8

(root@kali)-[~]
# rar2john test.rar > hash.txt

(root@kali)-[~] Kali自带的字典文件
# john hash.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (RAR5 [PBKDF2-SHA256 256/256 AVX2 8x])
Cost 1 (iteration count) is 32768 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
123456 (test.rar)
123456 (test.rar)
123456 (test.rar)
3g 0:00:00:21 DONE 2/3 (2023-11-15 21:40) 0.1428g/s 583.4p/s 583.4c/s 1750C/s 123456.. john
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

# 验证

