

实验吧训练题库-隐写术：九连环

原创

小白喵 于 2018-05-02 15:20:05 发布 3344 收藏 2

分类专栏：[学习记录](#)

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：<https://blog.csdn.net/zhou592930059/article/details/80166132>

版权



[学习记录](#) 专栏收录该内容

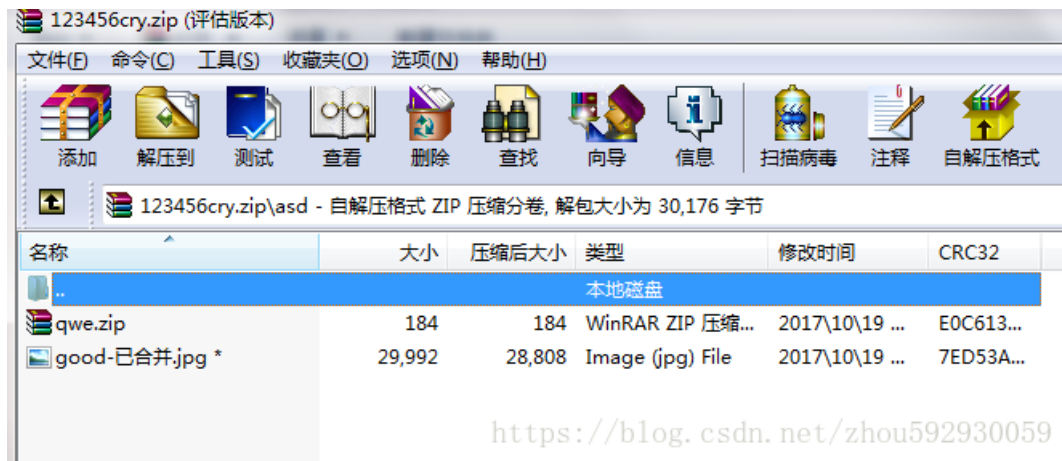
3 篇文章 0 订阅

订阅专栏

好记性不如烂笔头，学到的东西或者做过的练习最好记录一下，不然容易忘。

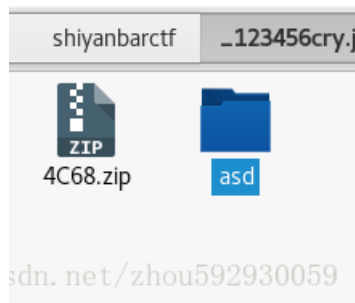
进入实验吧的练习题库，做题隐写术的题。题目：九连环

打开链接，是一张图片，下载到本地。一般情况下要改后缀名为.zip，用notepad打开验证一下，果然在最后看到.zip。然后改后缀，打开看一下里面都有什么，先不解压。



发现里面有一个压缩包和一张图片。但是，解压时让输入密码，看评论说密码还挺复杂，就不要破解了。我试着直接按回车键，解压出来一个名为asd的文件夹，打开发现里面是空的。

好吧，这样不行。打开kali系统，开网页存图片，因为知道里面有东西，所以直接用binwalk -e分解，分成一



个zip和那个asd文件夹。直接打开asd，里面同样有一张图片和一个压缩包

123456cry.jpg.extracted



，qwe直接提取，发现里面有一个flag.txt，但是需要密码，应该需要这张图片上找密码了。用stegsolve也没看到啥。用steghide试试

```
root@kali:~/桌面/shiyanbarctf/_123456cry.jpg.extracted/asd# steghide extract -sf
good-已合并.jpg
Enter passphrase:
wrote extracted data to "ko.txt".
root@kali:~/桌面/shiyanbarctf/_123456cry.jpg.extracted/asd#
```

<https://blog.csdn.net/zhou592930059>

出来一个ko.txt，里面是打开压缩包的密码。然后提取出flag.txt，就得到flag了。

如果用binwalk分解出来的图片是0字节，这样做：

- 1、卸载掉已有的binwalk。
- 2、打开<https://github.com/ReFirmLabs/binwalk>下载压缩包，安装命令github上写明了。安装好。
- 3、可以用了。如果在刚才的终端里运行不出来，关了重新开一个就可以了。