BUUCTF misc 九连环

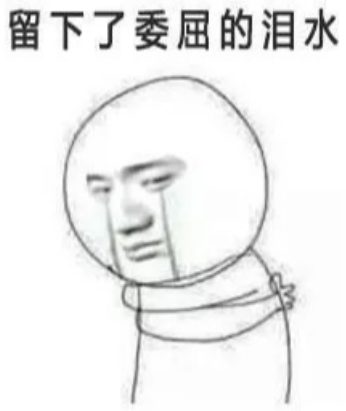
原创

Warning 于 2019-10-06 09:54:15 发布 5808 收藏 4
分类专栏： 杂项 工具 文章标签： steghide

涉及到的知识点：

- steghide的使用

题目一开始给了一张图片：



拿到winhex中去看，搜索文件尾FF D9，发现后面还有压缩包，于是丢到foremost中分离，果然分离出了一个压缩包，但是解压需要密码，我第一反应是这个图片的名字：

这……长得多像一个密码啊……

但是并不是。

然后我在winhex中手动分离了这个压缩包，（zip的文件头50 4B 03 04，结尾块标识50 4B 05 06）

发现居然没有密码了……居然是个伪加密吗……

好吧，然后解压出来了，里面有一个图片和一个压缩包，这个压缩包也是加密的，那密码大概率是从图片中来的，对着图片分析了一圈什么都没发现，binwalk，foremost也都说图片里面什么都没有……搞什么嘛

于是我又一次没有骨气地去看了wp，知道了一个神器：steghide，它也可以隐藏数据、文件到图片里，当然也可以用来提取，用法如下：（来源：https://blog.csdn.net/Blood_Seeker/article/details/81837571）

用法介绍：

embed, –embed embed data
extract, –extract extract data
-ef, –embedfile select file to be embedded
-ef （filename） embed the file filename
-cf, –coverfile select cover-file
-cf （filename） embed into the file filename
-p, –passphrase specify passphrase
-p （passphrase） use to embed data
-sf, –stegofile select stego file
-sf （filename） write result to filename instead of cover-file

用法示例：

将secret.txt文件隐藏到text.jpg中：
steghide embed -cf test.jpg -ef secret.txt -p 123456

从text.jpg解出secret.txt:
#steghide extract -sf test.jpg -p 123456

kali下安装：

```
apt-get install steghide
```

这道题没有设置密码，使用steghide需要输入密码时直接回车就好。果然用了之后，在提取出的ko.txt中发现了密码，解压后既可获得flag：