实验吧--隐写术--九连环--WriteUp

转载

weixin_30832143 于 2018-04-22 22:00:00 发布 234 收藏
原文链接：http://www.cnblogs.com/ESHLkangi/p/8909882.html

题目:

http://ctf5.shiyanbar.com/stega/huan/123456cry.jpg

是一张图：

放到binwalk查看一下

```
root@kali:~# binwalk ~/桌面/123456cry.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
19560         0x4C68          Zip archive data, at least v1.0 to extract, name:
asd/
48454         0xBD46          Zip archive data, at least v1.0 to extract, compre
ssed size: 184, uncompressed size: 184, name: asd/qwe.zip
48657         0xBE11          End of Zip archive
48962         0xBF42          End of Zip archive
```

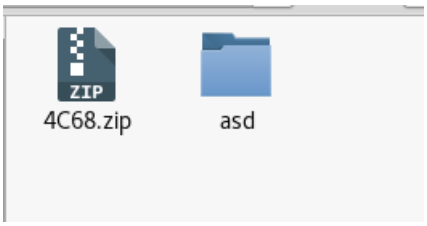
发现存在压缩文件。

使用-e参数将文件分离

```
root@kali:~# binwalk -e ~/桌面/123456cry.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
19560         0x4C68          Zip archive data, at least v1.0 to extract, name:
asd/
48454         0xBD46          Zip archive data, at least v1.0 to extract, compre
ssed size: 184, uncompressed size: 184, name: asd/qwe.zip
48657         0xBE11          End of Zip archive
48962         0xBF42          End of Zip archive
```

打开文件



4C68.zip和asb文件夹

压缩包和文件夹的内容是一样的，但是里面的图片不一样

压缩包的：

asb文件夹的：

这个图片是0KB的，不是我们想要的，因此压缩包里的才是我们想要的。

asb文件夹里面还有一个压缩包，里面有一个加密的flag.txt文件，就是我们的flag

怎么获取解压密码，就在图片里了。

想到的是4c68.zip可能是一个伪加密的zip，放到winhex看看

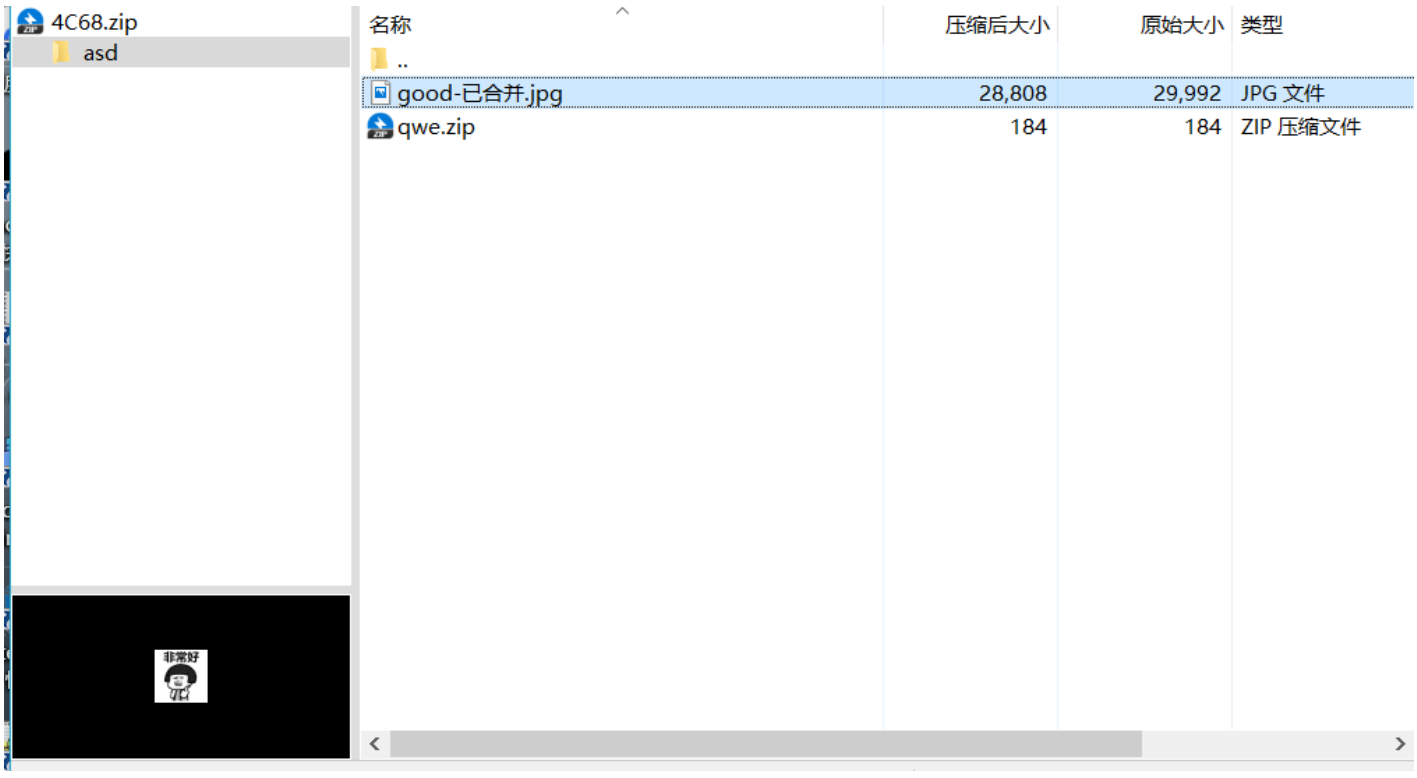
发现了，果然是伪加密

```
00007160  C4 35 B6 22 00 00 00 16  00 00 00 08 00 24 00 00
00007170  00 00 00 00 00 20 00 00  00 00 00 00 00 66 6C 61
00007180  67 2E 74 78 74 0A 00 20  00 00 00 00 00 01 00 18
00007190  00 29 39 FE E9 7C 48 D3  01 D9 46 44 DC 7C 48 D3
000071A0  01 D9 46 44 DC 7C 48 D3  01 50 4B 05 06 00 00 00
000071B0  00 01 00 01 00 5A 00 00  00 48 00 00 00 00 00 50
000071C0  4B 01 02 3F 00 0A 00 00  08 00 00 AE 54 53 4B 00
000071D0  00 00 00 00 00 00 00 00  00 00 00 04 00 24 00 00
000071E0  00 00 00 00 00 10 00 00  00 00 00 00 00 61 73 64
000071F0  2F 0A 00 20 00 00 00 00  00 01 00 18 00 69 B8 48
00007200  34 83 48 D3 01 69 B8 48  34 83 48 D3 01 E9 FC 59
00007210  31 83 48 D3 01 50 4B 01  02 3F 00 14 00 01 08 08
00007220  00 48 4E 53 4B 8C 3A D5  7E 88 70 00 00 28 75 00
00007230  00 16 00 24 00 00 00 00  00 00 00 20 00 00 00 22
00007240  00 00 00 61 73 64 2F 67  6F 6F 64 2D E5 B7 B2 E5
00007250  90 88 E5 B9 B6 2E 6A 70  67 0A 00 20 00 00 00 00
00007260  00 01 00 18 00 69 31 23  9C 7C 48 D3 01 29 AE F6
00007270  8F 82 48 D3 01 89 7E E8  D2 7C 48 D3 01 50 4B 01
```

将01改为00，保存

```
000071B0  00 01 00 01 00 5A 00 00  00 48 00 00 00 00 00 50
000071C0  4B 01 02 3F 00 0A 00 00  08 00 00 AE 54 53 4B 00
000071D0  00 00 00 00 00 00 00 00  00 00 00 04 00 24 00 00
000071E0  00 00 00 00 00 10 00 00  00 00 00 00 00 61 73 64
000071F0  2F 0A 00 20 00 00 00 00  00 01 00 18 00 69 B8 48
00007200  34 83 48 D3 01 69 B8 48  34 83 48 D3 01 E9 FC 59
00007210  31 83 48 D3 01 50 4B 01  02 3F 00 14 00 00 08 08
00007220  00 48 4E 53 4B 8C 3A D5  7E 88 70 00 00 28 75 00
00007230  00 16 00 24 00 00 00 00  00 00 00 20 00 00 00 22
00007240  00 00 00 61 73 64 2F 67  6F 6F 64 2D E5 B7 B2 E5
00007250  90 88 E5 B9 B6 2E 6A 70  67 0A 00 20 00 00 00 00
```

发现，可以解压了。



将good-已合并.jpg放到steghide工具检测一下，

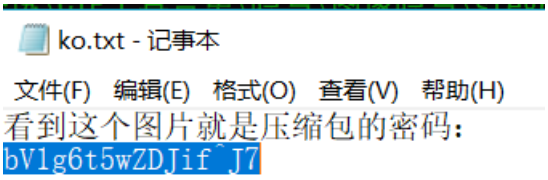
```
F:\[redacted]CTF工具合集\隐写\图像隐写\steghide>steghide.exe info good.jpg
"good.jpg":
  format: jpeg
  capacity: 1.2 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "ko.txt":
    size: 48.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes
```

发现了额外的数据

使用extract -sf 命令将隐藏式文件提取出来。

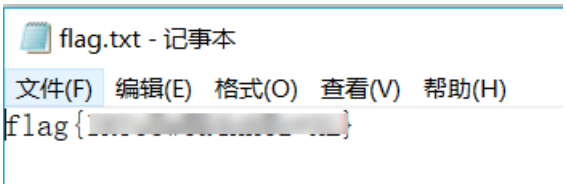
```
F:\[redacted]\CTF工具合集\隐写\图像隐写\steghide>steghide.exe extract -sf good.jpg
Enter passphrase:
wrote extracted data to "ko.txt".
```

打开ko.txt



获得解压密码

获得flag



转载于:https://www.cnblogs.com/ESHLkangi/p/8909882.html