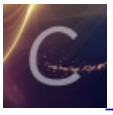
bugku-writeup-MISC-隐写2

原创

dark2019 于 2021-07-15 13:39:26 发布 69 收藏
分类专栏： 信息安全 wp 文章标签： 杂项 bugku 隐写


信息安全 同时被 2 个专栏收录
53 篇文章 1 订阅
订阅专栏


wp
31 篇文章 0 订阅
订阅专栏

题目：隐写2

工具：fcrackzip

binwalk

010 editor

base64在线解码工具： http://ctf.ssleye.com/base64.html

01—binwalk查看文件

```
binwalk -e yinxie2.jpg
```

使用kali中自带的binwalk查看文件，发现该文件为zip文件。

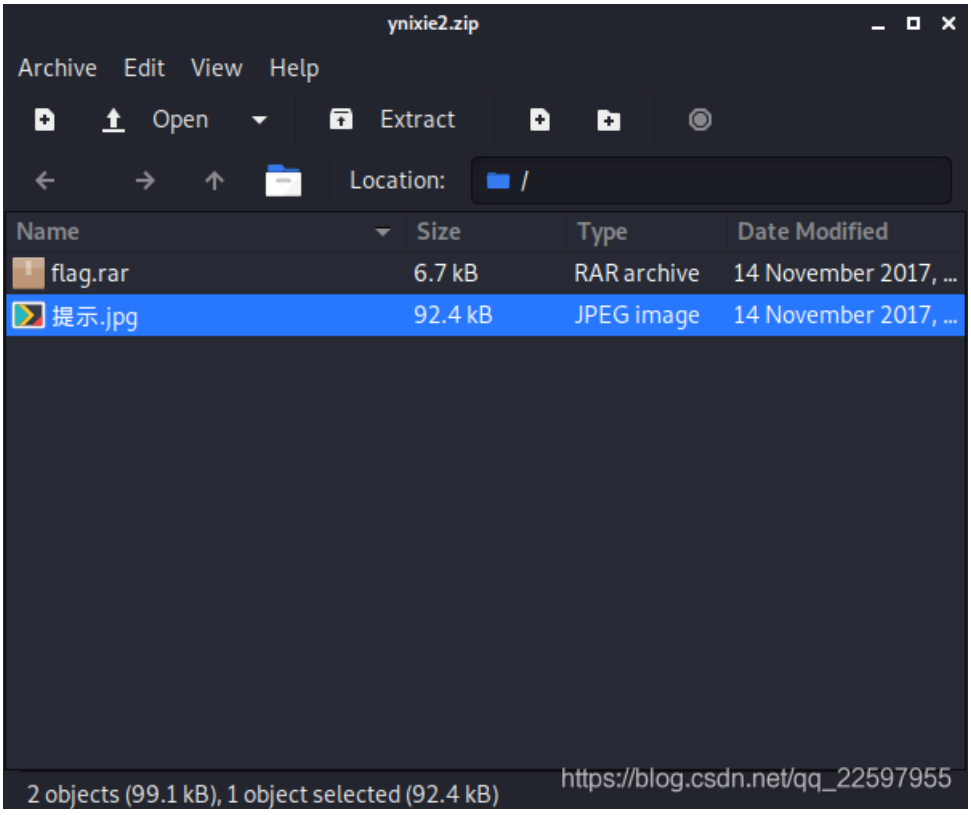
```
┌──(kali㉿kali)-[~]
└─$ binwalk -e yinxie2.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
30            0x1E            TIFF image data, big-endian, offset of first image directory: 8
52516         0xCD24          Zip archive data, at least v1.0 to extract, compressed size: 6732, uncompressed size: 6732, name: flag.rar
59264         0xE780          End of Zip archive, footer length: 22
147852        0x2418C         End of Zip archive, footer length: 22
```



```
dd if=yinxie2.jpg of=ynixie2.zip skip=52516 bs=1
```

使用binwalk命令转换为zip文件。

```
┌──(kali㉿kali)-[~]
└─$ dd if=yinxie2.jpg of=ynixie2.zip skip=52516 bs=1
95358+0 records in
95358+0 records out
95358 bytes (95 kB, 93 KiB) copied, 0.416004 s, 229 kB/s
```



告诉你们一个秘密，密码是3个数哦。

查理曼：
查理曼，法兰克王国国王，征服了西欧与中欧大部分土地，具有了至高无上的权威，下令全国人民信仰基督教，查理重振了西罗马帝国。
雅典娜：
女神帕拉斯·雅典娜，是希腊神话中的女战神也是智慧女神，雅典是以她命名的。
兰斯洛特，
英格兰传说中的人物，是亚瑟王圆桌骑士团中的一员。看上去就是一个清秀年轻的帅小伙儿，由于传说中他是一名出色的箭手，因此梅花J手持箭支。兰斯洛特与王后的恋爱导致了他与亚瑟王之间的战争。
Hint:
其实斗地主挺好玩的。

得到zip文件，查看**flag.rar**需要密码，再看看**提示.jpg**,提示密码为3个数。考虑使用爆破工具。

```
┌──(kali㉿kali)-[~]
└─$ fcrackzip -b -l 3-3 -c1 -v yinxie2/flag.rar
found file '3.jpg', (size cp/uc   6588/  6769, flags 801, chk 102c)
possible pw found: 035 ()
possible pw found: 337 ()
possible pw found: 728 ()
possible pw found: 871 ()
```

02—fcrackzip压缩文件密码爆破

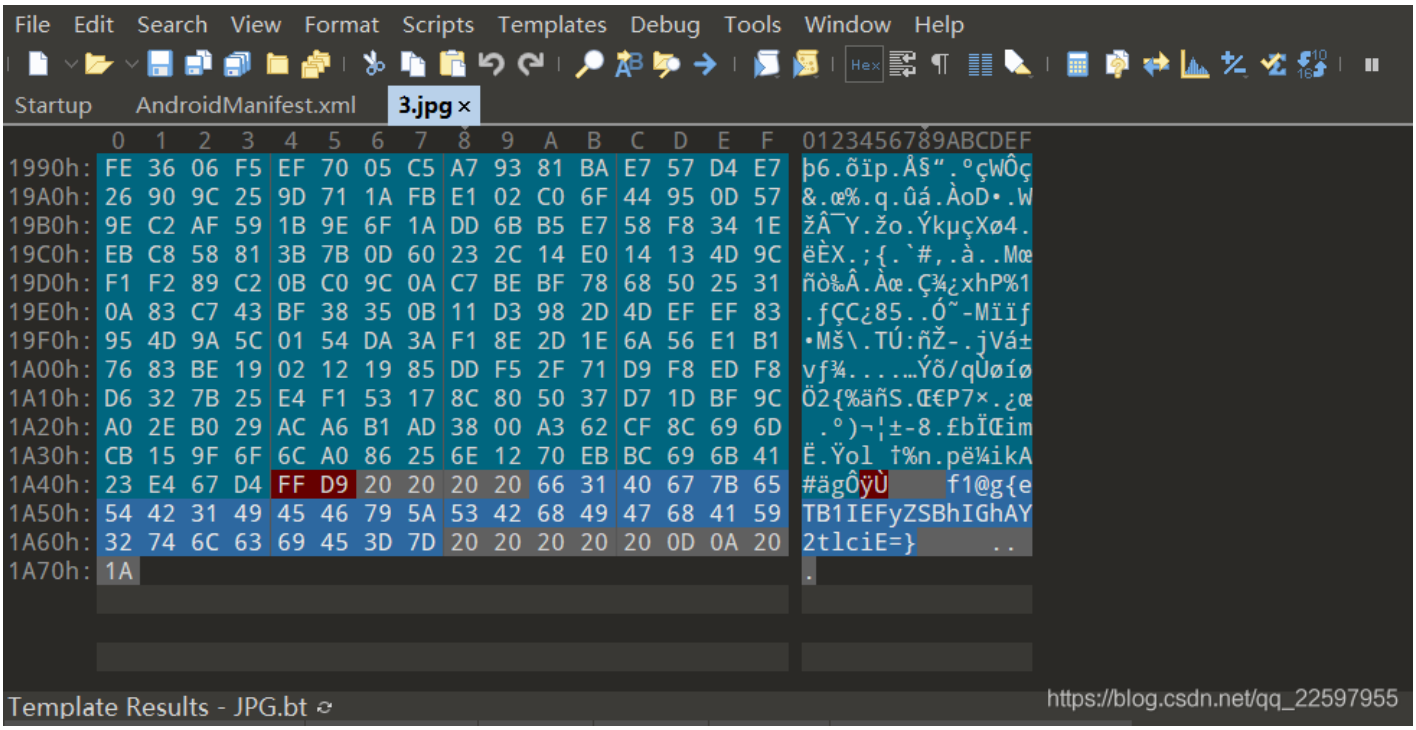
使用fcrackzip进行简单密码的爆破，kali中安装和使用链接：

https://blog.csdn.net/qq_22597955/article/details/118751974?spm=1001.2014.3001.5502

得到密码为871

输入密码，得到3.jpg图像如上所示。

03—010 editor 查看图片



使用010 editor查看图像3.jpg,文件末尾找到flag线索。

04—base64在线解码

尝试输入flag，发现错误，对其进行base64解码，得到正确flag。