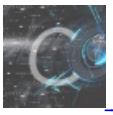
buuctf 刷新过的图片 F5隐写

原创

前方是否可导？ 于 2020-08-31 22:40:17 发布 681 收藏 1

分类专栏： Misc

本文链接：https://blog.csdn.net/weixin_44110537/article/details/108331146




```
root@mykali:~# git clone https://github.com/matthewgao/F5-steganography
正克隆到 'F5-steganography'...
remote: Enumerating objects: 64, done.
remote: Total 64 (delta 0), reused 0 (delta 0), pack-reused 64
展开对象中: 100% (64/64), 完成.
root@mykali:~# ls
attachment  Downloads          Music                Templates
biubiu.jpg  F5-steganography   Pictures             Videos
Desktop     Misc-encrypt       Public
Documents   Misc-encrypt.zip   setuptools-19.6.tar.gz
root@mykali:~# cd F5-steganography/
root@mykali:~/F5-steganography# java Extract ../Pictures/Misc.jpg
Huffman decoding starts
Permutation starts
309504 indices shuffled
Extraction starts
Length of embedded file: 190 bytes
(1, 31, 5) code used
root@mykali:~/F5-steganography# ls
bin.noise  e             Extract.class  james        Makefile  output.txt
crypt      e.bat         Extract.java   java         ms_d.bat  readme.md
d          Embed.class   gpl.txt        license.txt  ms_e.bat  sun
d.bat      Embed.java    image          lopez.bmp    ortega
root@mykali:~/F5-steganography#
```


安装完F5-steganography后找出output.txt

```
root@mykali:~/F5-steganography# cat output.txt
Pf??L<rEY(flag.txtK?IL??4KMK1H4206O10K361??L?4240?47?HM?Pf??L<rEY($ flag.txt
 ?0?????????k ?PKZNroot@mykali:~/F5-steganography#
```

发现是一个zip压缩包,接着猜测这个zip是个伪加密,winhex修改后直接打开.

flag{96efd0a2037d06f34199e921079778ee}