CTF-隐写术-我就是flag

原创

湖zz 于 2019-08-12 14:17:44 发布
文章标签： CTF 隐写术

题目:http://ctf5.shiyanbar.com/stega/bestwing12345678.bmp

1.用winhex查看图片,可以发现少了文件头
winhex直接编辑加上:

424D360C300000000000360000002800000056050000003000001001800000000000000000000000000000

或者用py脚本增加,以下为code:

```
def generate_bmp():
    bmp_header = b'\x42\x4d\x36\x0c\x30\x00\x00\x00\x00\x00' \
                 b'\x36\x00\x00\x00\x28\x00\x00\x00\x56\x05\x00' \
                 b'\x00\x00\x03\x00\x00\x01\x00\x18\x00\x00\x00' \
                 b'\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00' \
                 b'\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'

    new_bmp = b''
    with open('bestwing12345678.bmp', mode='rb')as f:
        new_bmp=f.read()

    with open('bmp.bmp', mode='wb') as f1:
        f1.write(bmp_header + new_bmp)


if __name__ == '__main__':
    generate_bmp()
    print('success')
```

2.打开bmp.bmp后发现图片很模糊,左上角应该是个二维码,然后中间是Key:filename
由此可知采用了某种加密方法，密匙为文件名
再看文件名为:bestwing12345678
刚好是个16位的字符串
于是猜测是AES加密

使用py直接解密:

```
import pyaes

def generate_bmp():
    bmp_header = b'\x42\x4d\x36\x0c\x30\x00\x00\x00\x00\x00' \
                 b'\x36\x00\x00\x00\x28\x00\x00\x00\x56\x05\x00' \
                 b'\x00\x00\x03\x00\x00\x01\x00\x18\x00\x00\x00' \
                 b'\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00' \
                 b'\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'
```

```
    key = b'bestwing12345678'
    new_bmp = b''
    with open('bestwing12345678.bmp', mode='rb')as f:
        byte_content = f.read()
        aes = pyaes.AESModeOfOperationECB(key)

        for i in range(0, len(byte_content), 16):
            byte16 = byte_content[i: i + 16]
            decrypt_byte = aes.decrypt(byte16)
            new_bmp += decrypt_byte
    with open('bmp2.bmp', mode='wb') as f1:
        f1.write(bmp_header + new_bmp)


if __name__ == '__main__':
    generate_bmp()
    print('success')
```

3.最终得到清晰的图片,上面存在二维码,直接扫描或者用py代码读取得到flag

py解析二维码:

```
import pyzbar.pyzbar as pyzbar
from PIL import Image,ImageEnhance

img = Image.open("bmp.bmp")

barcodes = pyzbar.decode(img)

for barcode in barcodes:
    barcodeData = barcode.data.decode("utf-8")
    print(barcodeData)
    print("success")
```

得到flag:flag{Swing_say_he11o_to_everyone}