问鼎杯四道Misc题

Misc1: 盲水印攻击

下载下来是一张cat.png的图片，用binwalk分析一下，发现存在zip压缩包，将压缩包提取出来

```
binwalk -e cat.png
```

在压缩包里面有两张图片day1.png, day2.png , 联想到之前国赛做过的盲水印攻击(两张图片), 工具在github上开源 `https://github.com/chishaxie/BlindWaterMark`

```
python bwm.py decode day1.png day2.png flag.png
```

Misc2: 词频分析

给了一段很长的看起来无规则的单词， 用在线词频分析一下就可以解出来flag了， 密文忘了 https://quipqiup.com/

Misc3 流量分析

用wireshark打开流量包, 文件->到处对象->到处HTTP, 有三条数据，其中有一个压缩包，保存下来后打开需要密码才能解开压缩包， 这时候我们先来看看流量包里面都有些啥，发现除了常见的tcp,udp,http,ssdp,ssh流量外还有telnet流量，我们知道telnet是明文传输的，因此追踪一些telent的tcp就可以发现很多数据了

```
[root@localhost wireshark]# llss

1  2  3  test
```

有四个文件，文件 1 内容是压缩包，文件 2 的内容为 `19aaFYsQQKr+hVX6hl2smAUQ5a767TsULEUebWSajEo=` , 文件 3 是一个加解密算法，因此我们知道文件 2 的内容为加密算法加密后的flag, 用解密算法还原一下就可以得到压缩包密码, 修改后的文件 3 内容如下

```python
# coding:utf-8
__author__ = 'YFP'
from Crypto import Random
from Crypto.Cipher import AES
import sys
import base64

help(AES)
IV = 'QWERTYUIOPASDFGH'
def decrypt(encrypted):
    aes = AES.new(IV, AES.MODE_CBC, IV)
    return aes.decrypt(encrypted)

def encrypt(message):
    length = 16
    count = len(message)
    padding = length - (count % length)
    message = message + '\0' * padding
    aes = AES.new(IV, AES.MODE_CBC, IV)
    return aes.encrypt(message)
# str = 'this is a test'
# example = encrypt(str)
example = "19aaFYsQQKr+hVX6hl2smAUQ5a767TsULEUebWSajEo="
example = example.decode('base64')
print(decrypt(example))
```

Misc4 二维码

下载下来是一个动态的gif， 先把每一帧提取下来，linux直接用命令`convert cake.gif test.png`，window下可以用stegsolve提取帧，一共四帧，仔细观察发现拼起来就是一张二维码了， 这里我们可以用ps，stegsolve的`Analyse->Image Combiner`功能，脚本这三种方法来合并 脚本为:

```
#!/usr/bin/env python
#coding:utf-8
from PIL import Image

im1 = Image.open('test-0.png')
im2 = Image.open('test-1.png')
im3 = Image.open('test-2.png')
im4 = Image.open('test-3.png')

print im1.size,im1.mode
width,height = im2.size
box1 = (0,0,width/2,height/2)
print box1
part1 = im1.crop(box1)
box2 = (width/2,0,width,height/2)
print box2
part2 = im2.crop(box2)
box3 = (0,height/2,width/2,height)
part3 = im3.crop(box3)
box4 = (width/2,height/2,width,height)
part4 = im4.crop(box4)

box = (450,450)

im = Image.new('L',box)
im.paste(part1,(0,0))
im.paste(part2,(225,0))
im.paste(part3,(0,225))
im.paste(part4,(225,225))
im.show()
```

用stegsolve得到的二维码需要再反色一下, 扫描得到一串16进制

```
03f30d0ab8c1aa596300000000000000000200000040000000732e000000
6400006401006c00005a00006402005a01006403005a0200640400840000
5a03006405008400005a040064010053280600000069ffffffff4e740300
0000637466733d0000003138362c39382c3138302c3135342c3133392c31
39322c3131342c31342c3130322c3136382c34332c3133362c35322c3231
382c38352c3130302c343363020000000400000007000000430000007361
0000007400006a01007c0100830100016401007d02007838007c0000445d
30007d03007c02007402007403007c03008301007400006a040064020064
03008302004183010064040017377d0200711a00577c02006a0500640400
8301007d02007c02005328050000004e7400000000690000000069ff0000
0074010000002c28060000007406000000726e646f6d74040000007365
6564740300000073747274030000006f7264740700000072616e64696e74
74050000007374726970280400000074040000007374723174030000006b
65797404000000737472327401000000632800000000280000000073 1000
00002f686f6d652f6374662f6262622e7079740500000066756e63310700
0000730c00000000010d0106010d012e010f016302000000040000000700
000043000000735d0000007400006a01007c0100830100016401007d0200
7843007c00006a0200640200830100445d32007d03007403007c03008301
007d03007c02007404007c03007400006a0500640300640400830200418 3
0100377d0200712300577c02005328050000004e52010000005202000000
690000000069ff0000002806000000520300000052040000007405000000
73706c697474030000006 96e747403000000636872520700000028040000
00520b000000520a00000052090000007401000000692800000000280000
00007310000000 2f686f6d652f6374662f6262622e70797405000000 6675
6e63320f000000730c00000000010d01060116010c012401280500000052
03000000520a00000074040000007374727252 0d0000005212000000 2800
0000002800000000280000000073100000002f686f6d652f6374662f6262
622e707974080000003c6d6f64756c653e0100000073080000000c020601
06030908
```

看到03f30d0a, 就大概知道这是一个pyc的文件头, 这里推荐一个查看各种文件头的网站 `https://en.wikipedia.org/wiki/List_of_file_signatures`
用010editor用edit->paste from->paste from hex粘贴为十六进制值，保存为pyc后缀文件, 然后利用 `uncompyle6 1.pyc > 1.py` (uncompyle6可以用pip安装 `pip install uncompyle6`)

解密后的内容为:（稍作修改），func2即为解密函数，不过这个脚本要在linux运行，因为window和linux的seed值不一样

```python
import random
key = 'ctf'
strr = '186,98,180,154,139,192,114,14,102,168,43,136,52,218,85,100,43'

def func1(str1, key):
    random.seed(key)
    str2 = ''
    for c in str1:
        str2 += str(ord(c) ^ random.randint(0, 255)) + ','

    str2 = str2.strip(',')
    return str2


def func2(str2, key):
    random.seed(key)
    str1 = ''
    for i in str2.split(','):
        i = int(i)
        str1 += chr(i ^ random.randint(0, 255))

    return str1

print func1(strr,key)
print func2(strr,key)
```