第8届山东省大学生网络安全竞赛 逆向 WP

原创

zsky_t 于 2019-11-08 23:26:20 发布 671 收藏

分类专栏： CTF 文章标签： CTF

本文链接：https://blog.csdn.net/l15263458908/article/details/102981174

RE1

题目给出了一个flag.pyc文件和out.txt文件， 一看就是反编译pyc文件，于是开始用uncompyle6开始反编译，发现提示是模数错误

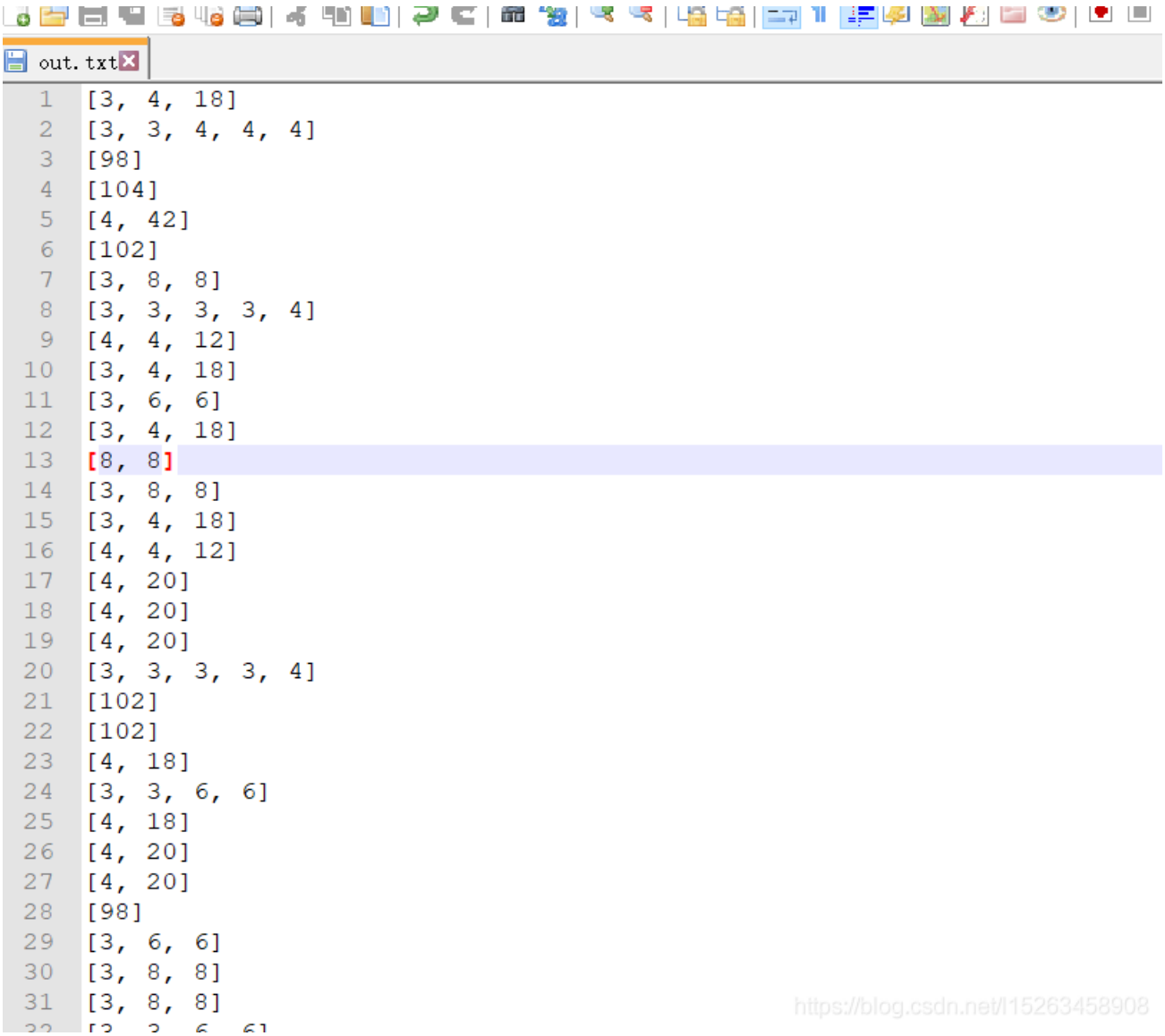
```
from_file_object
    float_version = float(magics.versions[magic][:3])
KeyError: b' \x19\r\n'

During handling of the above exception, another exception occurred:

Traceback (most recent call last):
  File "c:\users\19164\appdata\local\programs\python\python37\lib\runpy.py", line 193, in _run_module_as_main
    "__main__", mod_spec)
  File "c:\users\19164\appdata\local\programs\python\python37\lib\runpy.py", line 85, in _run_code
    exec(code, run_globals)
  File "C:\Users\19164\AppData\Local\Programs\Python\Python37\Scripts\uncompyle6.exe\__main__.py", line 9, in <module>
  File "c:\users\19164\appdata\local\programs\python\python37\lib\site-packages\uncompyle6\bin\uncompile.py", line 194
in main_bin
    **options)
  File "c:\users\19164\appdata\local\programs\python\python37\lib\site-packages\uncompyle6\main.py", line 261, in main
    source_encoding, linemap_stream, do_fragments)
  File "c:\users\19164\appdata\local\programs\python\python37\lib\site-packages\uncompyle6\main.py", line 161, in deco
ile_file
    source_size) = load_module(filename, code_objects)
  File "c:\users\19164\appdata\local\programs\python\python37\lib\site-packages\xdis\load.py", line 116, in load_modul
    get_code=get_code,
  File "c:\users\19164\appdata\local\programs\python\python37\lib\site-packages\xdis\load.py", line 152, in load_modul
from_file_object
    % (ord(magic[0:1]) + 256 * ord(magic[1:2]), filename)
ImportError: Unknown magic number 6432 in flag.pyc
```


于是打开文件发现模数是20 19，然后自己python2编译了对应的pyc文件，发现
模数是03 F3于是将模数修改，然后利用uncompyle6反编译出原py文件

```python
import math

flag = 'flag{********************}'
a = []
b = []
for i in flag:
    a.append(ord(i))

def func(para):
    res = True
    i = 2
    sq = int(math.sqrt(para)) + 1
    while i <= sq:
        if para % i == 0:
            b.append(i + 1)
            res = False
            func(para / i)
            i += 1
            break
        i += 1

    if res:
        b.append(para + 1)

for i in a:
    func(i)
    print b,
    b = []
```

然后观察输出，由于这里是func()由于时间关系，当时没来得及逆，于是直接写出所有的可能然后与结果去比对，最后得到flag

首先整理out.txt的格式为以下这种格式



```python
import math
import string


flag = ""
x = string.printable
a = []
b = []
for i in x:
    a.append(ord(i))

def func(para):
    res = True
    i = 2
    sq = int(math.sqrt(para)) + 1
    while i <= sq:
        if para % i == 0:
            b.append(i + 1)
            res = False
            func(para / i)
            i += 1
            break
        i += 1
    if res:
        b.append(para + 1)


dic = []
for i in a:
    func(i)
    dic.append((chr(i), str(b)))
    b = []

f = open("out.txt", "r")
lines = f.readlines()
print lines

for line in lines:
    for i in dic:
        if i[1] == line.strip().replace("\r\n", ""):
            flag +=  i[0]
            break

print flag
#flag{eb0cf2f1bfc9990ee3d399a2bbde3dd4}
```

RE2

拖入IDA观察，程序是需要输入10个字符，且范围是在“2356DESTZcqv”中，然后第一个字符和最后一个字符可以通过逻辑推出，中间8个是CRC爆破，通过下面和代码可以看出

```
.UPX1:004070B4                 ;org 4070B4h
.UPX1:004070B4                 align 8
.UPX1:004070B8 ; int dword_4070B8[251]
.UPX1:004070B8 dword_4070B8    dd 0, 77073096h, 0EE0E612Ch, 990951BAh, 76DC419h, 706AF48Fh
.UPX1:004070B8                                         ; DATA XREF: sub_401280+26↑r
.UPX1:004070B8                 dd 0E963A535h, 9E6495A3h, 0EDB8832h, 79DCB8A4h, 0E0D5E91Eh
.UPX1:004070B8                 dd 97D2D988h, 9B64C2Bh, 7EB17CBDh, 0E7B82D07h, 90BF1D91h
.UPX1:004070B8                 dd 1DB71064h, 6AB020F2h, 0F3B97148h, 84BE41DEh, 1ADAD47Dh
.UPX1:004070B8                 dd 6DDDE4EBh, 0F4D4B551h, 83D385C7h, 136C9856h, 646BA8C0h
.UPX1:004070B8                 dd 0FD62F97Ah, 8A65C9ECh, 14015C4Fh, 63066CD9h, 0FA0F3D63h
.UPX1:004070B8                 dd 8D080DF5h, 3B6E20C8h, 4C69105Eh, 0D56041E4h, 0A2677172h
.UPX1:004070B8                 dd 3C03E4D1h, 4B04D447h, 0D20D85FDh, 0A50AB56Bh, 35B5A8FAh
.UPX1:004070B8                 dd 42B2986Ch, 0DBBBC9D6h, 0ACBCF940h, 32D86CE3h, 45DF5C75h
.UPX1:004070B8                 dd 0DCD60DCFh, 0ABD13D59h, 26D930ACh, 51DE003Ah, 0C8D75180h
.UPX1:004070B8                 dd 0BFD06116h, 21B4F4B5h, 56B3C423h, 0CFBA9599h, 0B8BDA50Fh
.UPX1:004070B8                 dd 2802B89Eh, 5F058808h, 0C60CD9B2h, 0B10BE924h, 2F6F7C87h
.UPX1:004070B8                 dd 58684C11h, 0C1611DABh, 0B6662D3Dh, 76DC4190h, 1DB7106h
.UPX1:004070B8                 dd 98D220BCh, 0EFD5102Ah, 71B18589h, 6B6B51Fh, 9FBFE4A5h
.UPX1:004070B8                 dd 0E8B8D433h, 7807C9A2h, 0F00F934h, 9609A88Eh, 0E10E9818h
.UPX1:004070B8                 dd 7F6A0DBBh, 86D3D2Dh, 91646C97h, 0E6635C01h, 6B6B51F4h
.UPX1:004070B8                 dd 1C6C6162h, 856530D8h, 0F262004Eh, 6C0695EDh, 1B01A57Bh
.UPX1:004070B8                 dd 8208F4C1h, 0F50FC457h, 65B0D9C6h, 12B7E950h, 8BBEB8EAh
.UPX1:004070B8                 dd 0FCB9887Ch, 62DD1DDFh, 15DA2D49h, 8CD37CF3h, 0FBD44C65h
.UPX1:004070B8                 dd 4DB26158h, 3AB551CEh, 0A3BC0074h, 0D4BB30E2h, 4ADFA541h
.UPX1:004070B8                 dd 3DD895D7h, 0A4D1C46Dh, 0D3D6F4FBh, 4369E96Ah, 346ED9FCh
.UPX1:004070B8                 dd 0AD678846h, 0DA60B8D0h, 44042D73h, 33031DE5h, 0AA0A4C5Fh
```

然后写脚本爆破。，，，，，，当时做题的时候看到是CRC了，，，，但是没想到是通过爆破解，，毕竟是数据量是12＾8，。。，下面是解题爆破代码

```
import zlib

table = "2356DESTZcqv"
total = 0
for a in table:
    print("Tried: " + str(total))
    for b in table:
        for c in table:
            for d in table:
                for e in table:
                    for f in table:
                        for g in table:
                            for h in table:
                                temp = a + b + c + d + e + f + g + h
                                total += 1
                                if((zlib.crc32(temp) & 0xffffffff) == 0x5984f05e):
                                    print temp
                                    exit(0)
```

中间8位是 cqZS62vD

```
18                  exit(0)

PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL

Tried: 179159040
Tried: 214990848
Tried: 250822656
Tried: 286654464
Tried: 322486272
cqZS62vD
```



```
{
  v6 = (*(_BYTE *)(flag + 9) + 25) ^ 0x19;
  v28 = (*(_BYTE *)flag - 1) ^ 0x20;
```

然后第一位和最后一位
通过这里可以推出，拼起来加上flag{}就是最终的flag

RE3

这道题给出的是data.bin文件和一个exe文件，，，这道题当时直接没时间看了，，，，这是后头看大佬的WP复现了一波，，，用DIE查这个程序是加了UPX壳的，，但是用upx -d没脱掉，，，于是用ESP定律手脱，然后用ImportREC PE 修复了下导入表，，拖入IDA，找到main开始分析，，，

```
n name
_401000
_4010C0
ckflag
ain
ose
ad
lloc
_malloc
_40142C
vind
ll
ek
nit
t
it
exit
itterm
open
f 140
overview
```

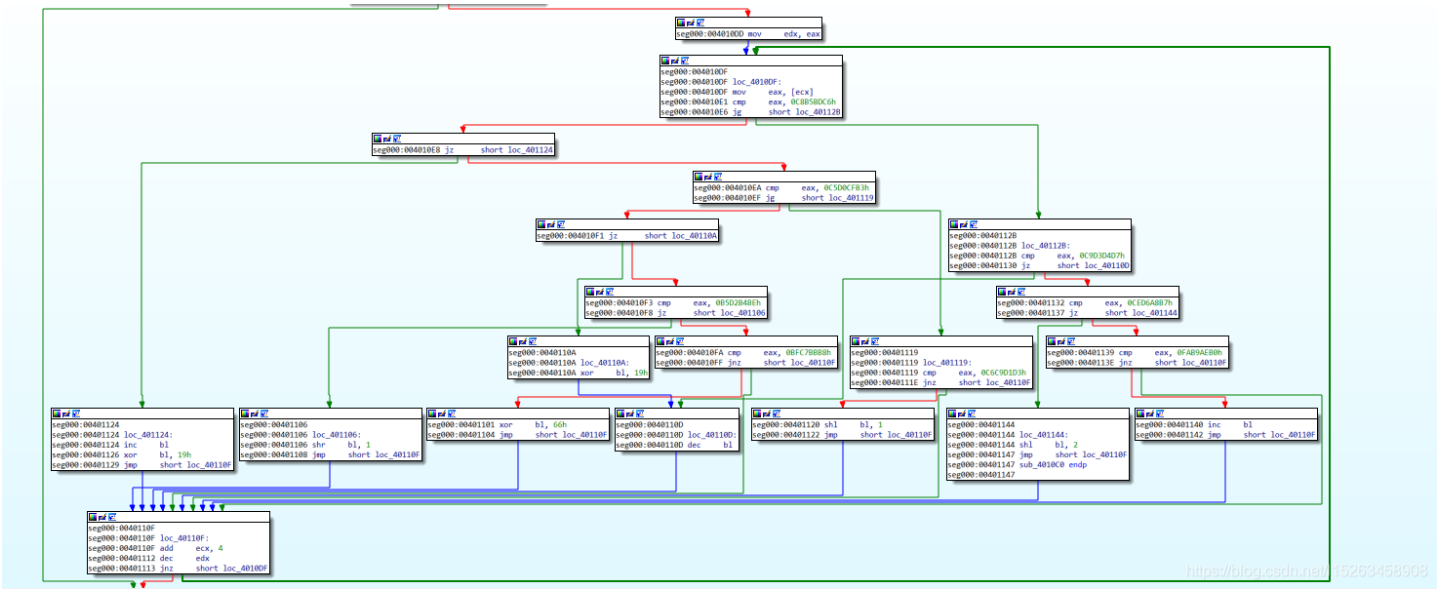
```
1  int __cdecl main(int argc, const char **argv, const char **envp)
2  {
3    int v3; // ST10_4
4    char flag; // [esp+4h] [ebp-34h]
5    char v6; // [esp+5h] [ebp-33h]
6    char v7; // [esp+35h] [ebp-3h]
7
8    flag = 0;
9    memset(&v6, 0, 0x30u);
10   v7 = 0;
11   sub_401000();
12   puts("\n      Hi,  SDNISC 2019 ~~~ \n\n");
13   printf((int)"serialNumber: ", v3);
14   scanf("%s", &flag);
15   if ( checkflag(&flag) == 1 )
16     puts("\n -->   Congratulations ~~~   <--\n");
17   else
18     puts("\n -->   Try again ~~~   <--\n");
19   return sub_40180D(0);
20 }
```


在sub_401000这个函数中，程序开始读取data.bin的数据，然后对byte_409064处的数据进行了xor 0x66

```
1  // write access to const memory has been detected, the output may be wrong!
2  int sub_401000()
3  {
4    FILE *v0; // eax
```

```
  5  FILE *v1; // esi
  6  char *v2; // edi
  7  signed int v3; // eax
  8
  9  v0 = fopen("data.bin", "rb");
 10  v1 = v0;
 11  if ( !v0 )
 12    exit(1);
 13  fseek(v0, 0, 2);
 14  dword_40B9F8 = ftell(v1);
 15  rewind(v1);
 16  v2 = (char *)malloc(0xAu);
 17  dword_40B9F4 = v2;
 18  if ( !v2 )
 19    exit(1);
 20  v3 = 0;
 21  do
 22  {
 23    byte_409064[v3] ^= 0x66u;
 24    ++v3;
 25  }
 26  while ( v3 < 32 );
 27  memset(v2, 0, 8u);
 28  memset(v2 + 8, 0, 2u);
 29  fread(0, 0u, 1u, v1);
 30  return fclose(v1);
 31}
```


来到 sub_4010C0函数



很明显的发现这是一道VM的逆向，然后opcode就是 data.bin中的每4个字节，
最后写脚本得到flag

```
import string
from pwn import *

a = [ 0x3B, 0x48, 0x2A, 0x53, 0x2F, 0x56, 0x60, 0x08, 0x11, 0x15,0x02, 0x56, 0x01, 0x14, 0x0E, 0x5A, 0x10, 0x33,
 0x3C, 0x34,   0x3E, 0x49, 0x1C, 0x5C, 0x35, 0x53, 0x3A, 0x1F, 0x4C, 0x17,   0x6F, 0x7A]

tar = [(x ^ 0x66) & 0xff  for x in a]


def fn1(x):
 return ((x+1)&0xff ^ 0x19)&0xff
```

```
def fn2(x):
 return (x>>1)&0xff
def fn3(x):
 return (x ^ 0x66)&0xff
def fn4(x):
 return (((x^0x19)&0xff) - 1)&0xff
def fn5(x):
    return (x-1)&0xff
def fn6(x):
 return (x << 1) &0xff
def fn7(x):
 return (x << 2)& 0xff
def fn8(x):
 return (x + 1) & 0xff


f = open("data.bin", "r")
data = f.read()
f.close()

op = []
for i in range(0, len(data), 4):
    y = u32(data[i:i+4])
    if y == 0xC8B5BDC6:
        op.append(fn1)
    elif y == 0xB5D2B4BE:
        op.append(fn2)
    elif y == 0xBFC7BBB8:
        op.append(fn3)
    elif y == 0xC5D0CFB3:
        op.append(fn4)
    elif y == 0xC9D3D4D7:
        op.append(fn5)
    elif y == 0xC6C9D1D3:
        op.append(fn6)
    elif y == 0xCED6A8B7:
        op.append(fn7)
    elif y == 0xFAB9AEB0:
        op.append(fn8)



flag = ""
s = string.printable

for i in range(32):
    for ss in s:
        if i % 2 == 0:
            sss = ord(ss) ^ 0x20
        else:
            sss = ord(ss) ^ 0x19
        for calc in op:
            sss = calc(sss)
        if sss == tar[i]:
            flag += ss
print flag
```

```
43          op.append(fn5)
44      elif y == 0xC6C9D1D3:
45          op.append(fn6)
46      elif y == 0xCED6A8B7:
47          op.append(fn7)
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL

```
root@kali:~# cd ./Desktop/
root@kali:~/Desktop# python dec.py
w5z6s7duQtR7AyFSTVhYv0H1m6JZxb33
root@kali:~/Desktop#
```


下面是3道题的链接

链接：https://pan.baidu.com/s/1L-J49h7m0xNDLAkCO_zMPA

提取码：3rp2

复制这段内容后打开百度网盘手机App，操作更方便哦