网鼎杯白虎组逆向writeup

原创

wumingpeng 于 2020-05-18 17:23:56 发布 310 收藏

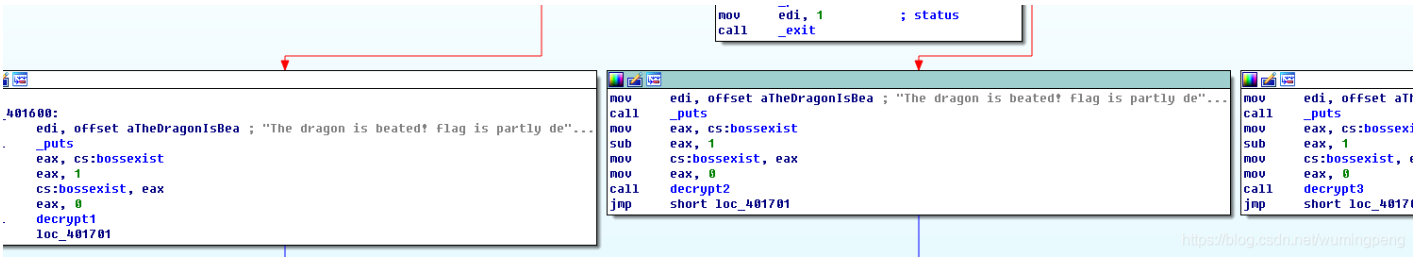
Hero

1flag格式如下

```
int outflag()
{
  byte_6034A8 = 0;
  byte_603484 = 0;
  byte_603489 = 0;
  byte_603444 = 0;
  byte_603449 = 0;
  byte_603468 = 0;
  return printf("flag{%s-%s-%s-%s-%s%s}", &unk_603445, flag3, flag1, flag2, &flag4, &unk_603485);
}
```

2几个flag分别在程序的几处赋值，如果正常走程序流程是到不了最后的

```
? x src
to filename? src.pyc
? x struc
to filename? struc
? x struct
to filename? struct
?
```



3调式运行程序，让程序跑起来，然后通过修改RIP寄存器的方式，跑到几个解密flag的函数出，最后在修改RIP跑到outflag函数。在内存中查看所有flag的数据并拼接起来。

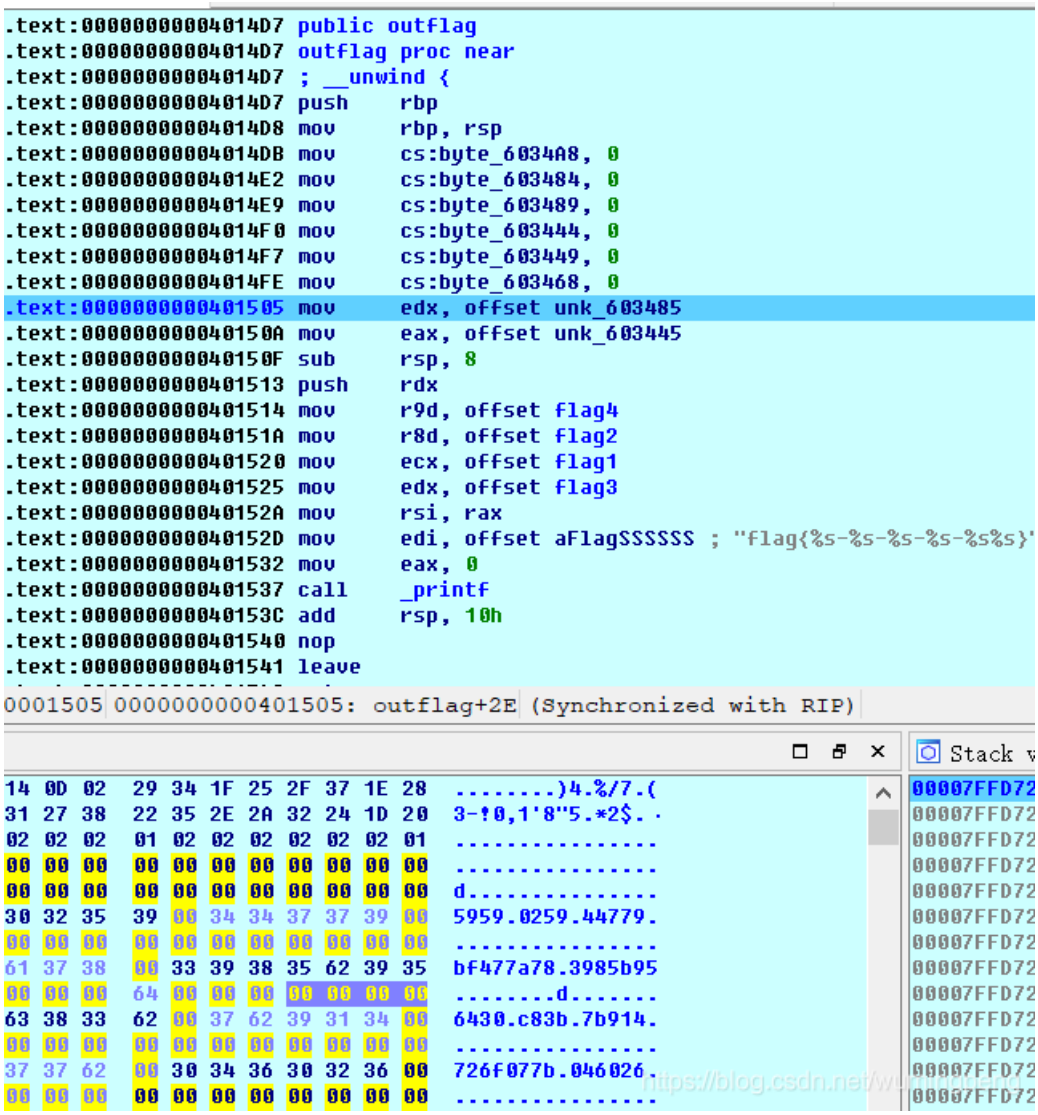
Flag1=726f077bf046026

Flag2=595910259844779

Flag3=6430dc83b17b914

Flag4= bf477a7893985b9

4 拼接flag,注意这几个flag中间被截断了



flag{0259-6430-726f077b-5959-bf477a78c83b}

src

1. 程序是python打包成的exe,需要重新反编译成pyc文件

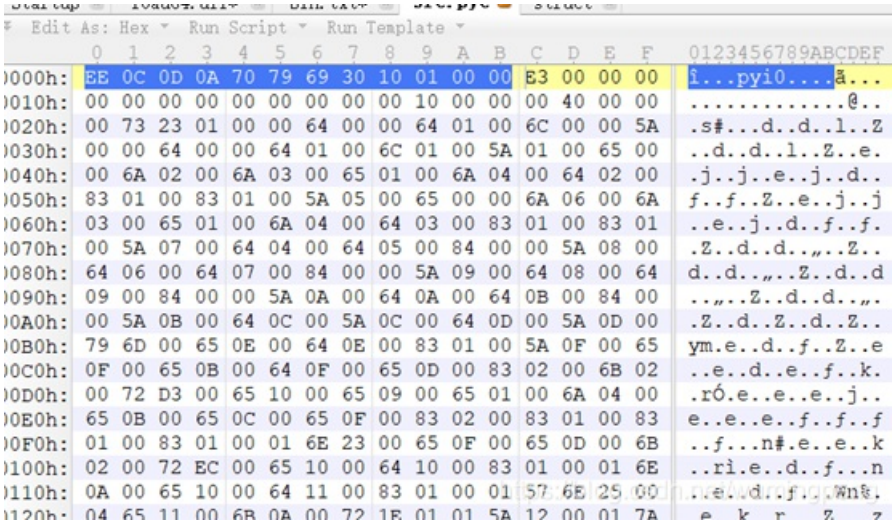
```
C:\Users\wmp10\Desktop\ctf\网鼎杯白虎组\ct>python archive_viewer.py src.exe
 pos, length, uncompressed, iscompressed, type, name
[(0, 269, 354, 1, 'm', 'struct'),
 (269, 1160, 2008, 1, 'm', 'pyimod01_os_path'),
 (1429, 4489, 10109, 1, 'm', 'pyimod02_archive'),
 (5918, 7600, 19806, 1, 'm', 'pyimod03_importers'),
 (13518, 1937, 4560, 1, 's', 'pyiboot01_bootstrap'),
 (15455, 1134, 1978, 1, 's', 'pyi_rth_multiprocessing'),
 (16589, 3512, 4966, 1, 's', 'src'),
 (20101, 298516, 328528, 1, 'b', 'MSVCR100.dll'),
 (318617, 25864, 28160, 1, 'b', '_bz2.pyd'),
 (344481, 33574, 35840, 1, 'b', '_ctypes.pyd'),
 (378055, 325761, 327680, 1, 'b', '_hashlib.pyd'),
 (703816, 67398, 69632, 1, 'b', '_lzma.pyd'),
 (771214, 7372, 9728, 1, 'b', '_multiprocessing.pyd'),
 (778586, 19233, 21504, 1, 'b', '_socket.pyd'),
 (797819, 475904, 478208, 1, 'b', '_ssl.pyd'),
 (1273723, 48607, 50688, 1, 'b', 'pyexpat.pyd'),
 (1322330, 903235, 929792, 1, 'b', 'python34.dll'),
 (2225565, 5054, 9728, 1, 'b', 'select.pyd'),
 (2230619, 375, 695, 1, 'b', 'src.exe.manifest'),
 (2230994, 206078, 208384, 1, 'b', 'unicodedata.pyd'),
 (2437072, 0, 0, 0, 'o', 'pyi-windows-manifest-filename src.exe.manifest'),
 (2437072, 6562, 21821, 1, 'x', 'Include\\pyconfig.h'),
 (2443634, 205414, 766529, 1, 'x', 'base_library.zip'),
 (2649048, 1373664, 1373664, 0, 'z', 'PYZ-00.pyz')]
?
```


2 提取出文件

```
? x src
to filename? src.pyc
? x struc
to filename? struc
? x struct
to filename? struct
?
```

src.exe_extracted	2020/5
archive_viewer.py	2020/5
src.pyc	2020/5
pyinstxtractor.py	2020/5
src.exe	2020/4
struct	2020/5

3 修复pyc文件



4用工具反编译出原代码