

网鼎杯白虎组逆向writeup

原创

wumingpeng



于 2020-05-18 17:23:56 发布



310



收藏

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) 版权协议，转载请附上原文出处链接和本声明。

本文链接：<https://blog.csdn.net/wumingpeng/article/details/106197418>

版权

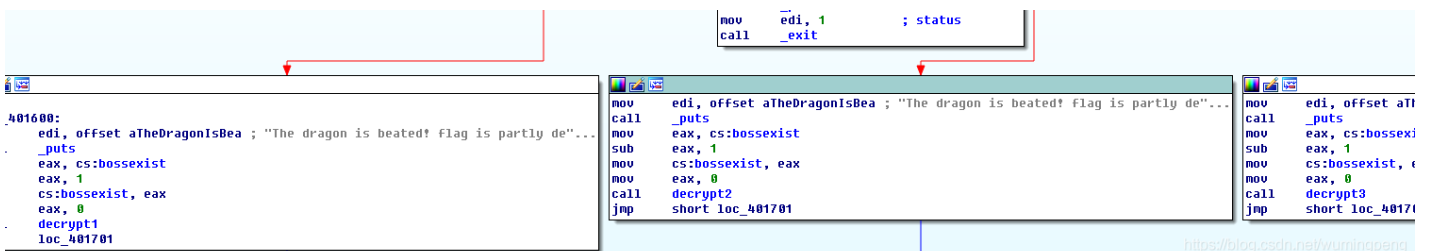
Hero

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}", &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

```
(2049048, 1575004, 1575004, 0, 2,
? 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

```
.text:00000000004014D7 public outflag
.text:00000000004014D7 outflag proc near
.text:00000000004014D7 ;__ unwind {
.text:00000000004014D7 push rbp
.text:00000000004014D8 mov rbp, rsp
.text:00000000004014DB mov cs:byte_6034A8, 0
.text:00000000004014E2 mov cs:byte_603484, 0
.text:00000000004014E9 mov cs:byte_603489, 0
.text:00000000004014F0 mov cs:byte_603444, 0
.text:00000000004014F7 mov cs:byte_603449, 0
.text:00000000004014FE mov cs:byte_603468, 0
.text:0000000000401505 mov edx, offset unk_603485
.text:000000000040150A mov eax, offset unk_603445
.text:000000000040150F sub rsp, 8
.text:0000000000401513 push rdx
.text:0000000000401514 mov r9d, offset flag4
.text:000000000040151A mov r8d, offset flag2
.text:0000000000401520 mov ecx, offset flag1
.text:0000000000401525 mov edx, offset flag3
.text:000000000040152A mov rsi, rax
.text:000000000040152D mov edi, offset aFlagSSSSSS ; "flag{%s-%s-%s-%s-%s}"
.text:0000000000401532 mov eax, 0
.text:0000000000401537 call _printf
.text:000000000040153C add rsp, 10h
.text:0000000000401540 nop
.text:0000000000401541 leave
-----
0001505 0000000000401505: outflag+2E (Synchronized with RIP)
```

14 00 02 29 34 1F 25 2F 37 1E 28)4.%/7.(00007FFD72
31 27 38 22 35 2E 2A 32 24 1D 20	3-!0,1'8"5.*2\$. .	00007FFD72
02 02 02 01 02 02 02 02 02 01	00007FFD72
00 00 00 00 00 00 00 00 00 00	00007FFD72
00 00 00 00 00 00 00 00 00 00	d.....	00007FFD72
30 32 35 39 00 34 34 37 37 39 00	5959.0259.44779.	00007FFD72
00 00 00 00 00 00 00 00 00 00	00007FFD72
61 37 38 00 33 39 38 35 62 39 35	bf477a78.3985b95	00007FFD72
00 00 00 64 00 00 00 00 00 00d.....	00007FFD72
63 38 33 62 00 37 62 39 31 34 00	6430.c83b.7b914.	00007FFD72
00 00 00 00 00 00 00 00 00 00	00007FFD72
37 37 62 00 30 34 36 30 32 36 00	726f077b.046026.	00007FFD72
00 00 00 00 00 00 00 00 00 00	00007FFD72

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')]
https://blog.csdn.net/wumingpeng
```

2 提取出文件

```
(2649048, 1373664, 1373664, 0, 'z', 'PYZ-00.pyz')
? 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

<https://blog.csdn.net/wumingpeng>

3 修复pyc文件

```
0000h: EE 0C 0D 0A 70 79 69 30 10 01 00 00 E3 00 00 00 i...pyi0...ã...
0010h: 00 00 00 00 00 00 00 00 00 10 00 00 00 40 00 00 .....@..
0020h: 00 73 23 01 00 00 64 00 00 64 01 00 6C 00 00 5A .s#...d..d..l..Z
0030h: 00 00 64 00 00 64 01 00 6C 01 00 5A 01 00 65 00 ..d..d..l..Z..e.
0040h: 00 6A 02 00 6A 03 00 65 01 00 6A 04 00 64 02 00 .j..j..e..j..d..
0050h: 83 01 00 83 01 00 5A 05 00 65 00 00 6A 06 00 6A f..f..Z..e..j..j
0060h: 03 00 65 01 00 6A 04 00 64 03 00 83 01 00 83 01 ..e..j..d..f..f.
0070h: 00 5A 07 00 64 04 00 64 05 00 84 00 00 5A 08 00 .Z..d..d...Z..
0080h: 64 06 00 64 07 00 84 00 00 5A 09 00 64 08 00 64 d..d...Z..d..d
0090h: 09 00 84 00 00 5A 0A 00 64 0A 00 64 0B 00 84 00 ....Z..d..d...
00A0h: 00 5A 0B 00 64 0C 00 5A 0C 00 64 0D 00 5A 0D 00 .Z..d..Z..d..Z..
00B0h: 79 6D 00 65 0E 00 64 0E 00 83 01 00 5A 0F 00 65 ym.e..d..f..Z..e
00C0h: 0F 00 65 0B 00 64 0F 00 65 0D 00 83 02 00 6B 02 ..e..d..e..f..k.
00D0h: 00 72 D3 00 65 10 00 65 09 00 65 01 00 6A 04 00 .ró.e..e..e..j..
00E0h: 65 0B 00 65 0C 00 65 0F 00 83 02 00 83 01 00 83 e..e..e..f..f..f
00F0h: 01 00 83 01 00 01 6E 23 00 65 0F 00 65 0D 00 6B ..f...n#e..e..k
0100h: 02 00 72 EC 00 65 10 00 64 10 00 83 01 00 01 6E ..ri.e..d..f...n
0110h: 0A 00 65 10 00 64 11 00 83 01 00 01 57 6E 25 00 .re/d..f..g..wng.
0120h: 04 65 11 00 6B 0A 00 72 1E 01 01 5A 12 00 01 7A e k r z z
```

4用工具反编译出原代码

