171125 逆向-湖湘杯RE

原创

奈沙夜影 于 2017-11-28 23:14:50 发布 457 收藏

分类专栏： CTF

本文链接：https://blog.csdn.net/whklhhhh/article/details/78660484

1625-5 王子昂 总结《2017年11月25日》【连续第421天总结】

A. 湖湘杯Re-WriteUp

B.

Re4newer

查壳发现加了UPX，脱壳机操作以后无法运行，于是直接静态分析

查找字符串锁定这里

```
1  int __usercall sub_401160@<eax>(char a1@<sil>)
2  {
3    int v1; // eax@1
4    int v2; // ecx@1
5    int v3; // ecx@3
6    signed int v4; // eax@5
7    char v6; // [sp+0h] [bp-3F4h]@1
8    char input; // [sp+8h] [bp-3ECh]@7
9
10   sub_4087D0(&v6);
11   v1 = sub_408A9C(&v6);
12   v2 = *(_DWORD *)(v1 + 20) + 1900;
13   if ( v2 > 2051 && v2 < 2053 )
14   {
15     v3 = *(_DWORD *)(v1 + 16) + 1;
16     if ( v3 > 2 && v3 < 4 )
17     {
18       v4 = *(_DWORD *)(v1 + 12);
19       if ( v4 > 13 && v4 < 15 )
20       {
21         sub_401020("Input your flag:", v6);
22         sub_401050("%s", &input);
23         check(strlen(&input), (int)&input, a1);
24       }
25     }
26   }
27   return 0;
28 }
```


再看内部校验：

```
15
16   v4 = xmmword_41D740;
17   v5 = xmmword_41D730;
18   v6 = xmmword_41D7A0;
19   v7 = xmmword_41D760;
20   v8 = xmmword_41D7D0;
21   v9 = xmmword_41D750;
22   v10 = xmmword_41D790;
23   v11 = xmmword_41D780;
```

```
24  v12 = xmmword_41D7C0;
25  v13 = xmmword_41D7B0;
26  v14 = xmmword_41D770;
27  if ( a1 == 44 )                               // 长度为44
28  {
29    i = 0;
30    do
31    {
32      if ( (*(_BYTE *)(i + a2) ^ 0x22) != *((_DWORD *)&v4 + i) )
33        break;
34      ++i;
35    }
36    while ( i < 44 );
37    if ( i == 44 )
38      sub_401020("success!\n", a3);
39    else
40      sub_401020("wrong~\n", a3);
41  }
42}
```


很简单的异或，只不过硬编码的顺序有一些变换，在脚本中相应处理即可：

```
dic = [4, 3, 0xA, 6, 0xD, 5, 9, 8, 0xC, 0xB, 7]

n = [89, 118, 74, 19, 68, 78, 67, 69, 81, 75, 79, 82, 125, 99, 125, 84, 125, 19, 86, 95, 112, 112, 103, 103, 78, 71, 125, 112, 81, 125, 75, 113, 82, 99, 81, 113, 103, 125, 87, 125, 17, 80, 91, 125]
for k in dic:
    k = k-3
    a = n[k*4:k*4+4]
    for i in a:
        print(chr(i^0x22), end='')
```

```
运行 re1
E:\Users\hasee\AppData\Local\Programs\Python\Python35-32\python.exe F:/ctf/hxb/re1.py
flag{Th1s_iS_A_v3ry_simple_RRREEE_u_pAsS_1t}
进程已结束,退出代码0
```


简单的Android

直接反编译，看到明码flag，提交完成

```
iput-object v0, p0, Lcom/wnagzihxain/application/MainActivity;->RegCode:Ljava/la

.line 13
const-string v0, "flag{Start_4ndr0id_Crack1ng_w1th_m3}"

iput-object v0, p0, Lcom/wnagzihxain/application/MainActivity;->Flag:Ljava/lang/
```


pyc分析

XDCTF2015的re300的原题，百度可以看到更详细的逆向分析

拖入网站在线反编译，再经过美化以后得到稍微能看的原脚本：

```
bbbb = (lambda __g, __y: [
    [
        [
            [
                [
                    [(fin.close(), [
                        [(lambda __items, __after, __sentinel: __y(lambda __this: lambda: (lambda __i: [(ss.append(c), (sss.append(0), __this())[1])[1]
                            for __g['c'] in [__i]
                        ][0]
                        if __i is not __sentinel
                        else __after())(next(__items, __sentinel)))())(iter(s), lambda: [
                        [(lambda __items, __after, __sentinel: __y(lambda __this: lambda: (lambda __i: [(lambda __value: [__this() for __g['sssss'] in [(lambda __ret: __g['sssss'] + __value
                            if __ret is NotImplemented
                            else __ret)(getattr(__g['sssss'], '__iadd__', lambda other: NotImplemented)(__value))]][0])(chr(c)) for __g['c'] in [__i]][0]
                        if __i is not __sentinel
                        else __after())(next(__items, __sentinel)))())(iter(ssss), lambda: [(fout.write(sssss), (fout.close(), None)[1])[1]
                        for __g['fout'] in [open('key.enc', 'wb+')]
                        ][0], []) for __g['sssss'] in ['']][0]
                        for __g['ssss'] in [encode(ss, sss)]
                    ][0], []) for __g['sss'] in [
                        []
                    ]][0]
```


用力反编译，发现脚本将每个字节在table中的index+1后，取低六位保存
于是解码脚本只需要取6位反查到table中的index-1的值输出即可
但是由于第7位在保存过程中丢失，因此需要写出两种情况进行对比参考：

```
    a=s//16
    b=(s>>8) & 0xFF
    c=s & 0xff
    sa=tobin(a)
    sb=tobin(b)
    sc=tobin(c)
    return table[int(sa[2:],2)]+table[int(sb[4:]+sa[:2],2)]+table[int(sc[6:]+sb[:4],2)]+table[int(sc[:6],2)]

a=open('key.enc','rb')
a=a.read()
s=''
for i in xrange(0, len(a), 3):
    s += decode(int(a[i:i + 3].encode('hex'), 16))
print(s)
# s = ''.join(map(lambda c: table[(table.index(c) + 63) % 64], s))
#
# print(s)
for i in s:
    sys.stdout.write(table[(find(i, table) - 1) % len(table)])
print()
for i in s:
    sys.stdout.write(table[(find(i, table) - 1 + 64) % len(table)])
```

运行 re3_re

```
E:\Python27\python.exe F:/ctf/hxb/re3/re3_re.py
0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ!"#$%&' ()*+,-./:;<=>?@[\]^_`{|}~
iiiiirrrrLfzea844d181c3249f6gtttgggggggg0000000000000
hhhhhqqqqKeyd9733c070b2138e5fsssfffffff^^^^^^^^^^^^^^()
>>>>>{{{{g;4:,*&&/#*#.%$&+;(<}}}<<<<<<<""""""""""""""
```


得到最终flag：

`>>>>>{{{{Key:9733c070b2138e5f}}}<<<<<<<`

C. 明日计划

湖湘杯部分MiscWP