南邮CTF逆向题第六道WxyV2解题思路

原创

iqiqiya 于 2017-12-24 11:42:29 发布 757 收藏
分类专栏： ------南邮CTF 我的CTF进阶之路 文章标签： 南邮CTF writeup 逆向 WxyV2 CTF

本文链接：https://blog.csdn.net/xiangshangbashaonian/article/details/78884187

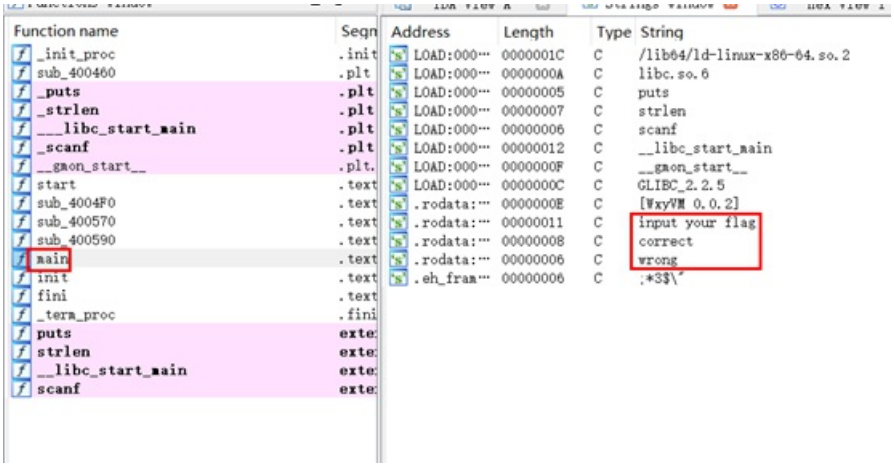
如题

看提示应该与第四道题WxyVM一样是ELF文件 那么我们直接上IDAx64

http://blog.csdn.net/xiangshangbashaonian/article/details/78883486

首先找到main函数

还是习惯性查看下可疑字符串



按下F5查看伪代码（中间有大段 我省略截图了）

```
__int64 __fastcall main(__int64 a1, char **a2, char **a3)
{
  char v4; // [sp+Bh] [bp-5h]@1
  signed int i; // [sp+Ch] [bp-4h]@3

  puts("[WxyVM 0.0.2]");
  puts("input your flag:");
  scanf("%s", &byte_694100);
  v4 = 1;
  if ( strlen(&byte_694100) != 25 )
    v4 = 0;
  dword_694140 = -1677284711;
  byte_694117 += 11;
  byte_694103 += 31;
  dword_69417C ^= dword_694178;
  dword_694180 ^= dword_69417C;
  dword_694184 ^= dword_694180;
  dword_694188 ^= dword_694184;
  dword_69418C ^= dword_694188;
  dword_694190 ^= dword_69418C;
  dword_694194 ^= dword_694190;
  dword_6941B4 ^= dword_6941B0;
```

```
  dword_6941E0 ^= dword_6941DC;
  byte_694102 ^= 0xBu;
  byte_694100 ^= 0x5Eu;
  byte_694111 += 69;
  byte_694109 += 7;
  for ( i = 0; i <= 24; ++i )
  {
    if ( *(&byte_694100 + i) != dword_694060[i] )
      v4 = 0;
  }
  if ( v4 )
    puts("correct");
  else
    puts("wrong");
  return 0LL;
}
```

这次就不一行一行分析了 大致意思是：

获取一个字符串存放到地址694100处

限制长度为25

那么如果要对这个字符串进行操作 只会从694100进行相应操作 那么其他的自然就是混淆我们 又可以清楚的看到 有效的操作都是以byte型进行 那么dword的我们直接过滤掉即可

```
过滤前:
dword_694140 = -1677284711;

byte_694117 += 11;

byte_694103 += 31;

dword_69417C ^= dword_694178;

dword_694180 ^= dword_69417C;

dword_694184 ^= dword_694180;

dword_694188 ^= dword_694184;

dword_69418C ^= dword_694188;

dword_694190 ^= dword_69418C;

dword_694194 ^= dword_694190;

dword_6941B4 ^= dword_6941B0;

dword_6941B8 ^= dword_6941B4;

dword_6941BC ^= dword_6941B8;

dword_6941C0 ^= dword_6941BC;
```

```
过滤后:
17 += 11

03 += 31

05 += 78

17 += 109

02 -= 25

01 -= 48

0B += 123

0D ^= 0x26

17 ^= 0x59

0C += 3

0B -= 5

0D += 75

04 ^= 0x48

05 -= 88
```

a

```
=[0xffffffC0,0xffffff85,0xffffffF9,0x6C,0xffffffE2,0x14,0xffffffBB,0xfffffffe4,0xd,0x59,0x1c,0x23,0xffffff88,0x
```

```
f = open('key.txt')#过滤后的txt文本自增自减的直接格式改下

for b in f.readlines()[::-1]:

if b[3]=='+':

if'x'in b:

a[int(b[:2],16)]-= int(b[8:],16if'x'in b else10)

else:

a[int(b[:2],16)]-= int(b[6:],10)
```

```
if b[3]=='-':

if'x'in b:

a[int(b[:2],16)]+= int(b[8:],16)

else:

a[int(b[:2],16)]+= int(b[6:],10)

if b[3]=='^':

if'x'in b:

a[int(b[:2],16)]^= int(b[8:],16)

else:

a[int(b[:2],16)]^= int(b[6:],10)

flag =""

for i in a:

flag += chr(i%256)

print flag
```

flag：nctf{th3_vM_w1th0ut_dAta}