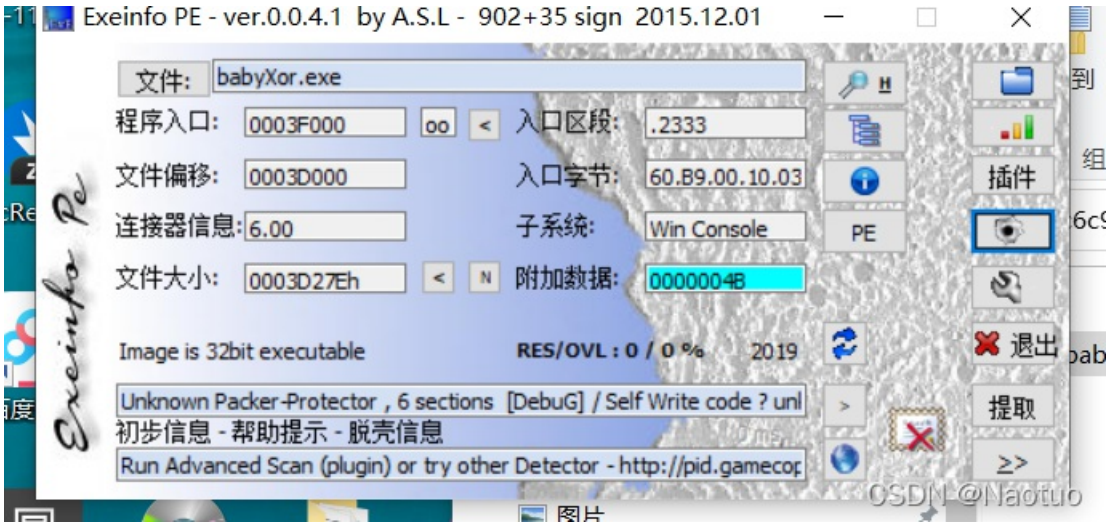
XCTF----babyxor

原创

Mov1A 于 2022-03-19 14:47:38 发布 28 收藏
分类专栏： CTF 文章标签： 其他

1。拿到文件，进行查壳



未知壳，使用OD进行手动脱壳（ESP定律法脱壳---- (20条消息) 破解入门（五）-----实战"ESP定律法"脱壳_lelexin的博客-CSDN博客）

2.脱壳后，拖入IDA进行分析

```
4  int v5; // [esp+50h] [ebp-1Ch]
5  void *v6; // [esp+54h] [ebp-18h]
6  const char *Src; // [esp+58h] [ebp-14h]
7  int v8; // [esp+5Ch] [ebp-10h]
8
9  sub_4010B4((int)&unk_4395F0, (char *)&byte_432020);
10 sub_40107D(sub_40102D);
11 if ( --File._cnt < 0 )
12   _filbuf(&File);
13 else
14   ++File._ptr;
15 v8 = sub_40108C(&unk_435DC0, 56);
16 Src = (const char *)sub_401041((int)&unk_435DC0, (int)&dword_435DF8, 56u);
17 v6 = malloc(0x64u);
18 v3 = strlen(Src);
19 memcpy(v6, Src, v3);
20 v5 = sub_4010C3((int)&unk_435DC0, (int)Src, (int)&dword_435E30, 56);
21 sub_40101E(v8, (int)Src, v5);
22 return 0;
23 }
```

代码并不复杂，直接上脚本

```
a1=[0x66,0x6d,0x63,0x64,0x7f,0x37,0x35,0x30,0x30,0x6b,0x3a,0x3c,0x3b,0x20]
a2=[0x37,0x6f,0x38,0x62,0x36,0x7c,0x37,0x33,0x34,0x76,0x33,0x62,0x64,0x7a]
a3=[0x1a,0,0,0x51,0x5,0x11,0x54,0x56,0x55,0x59,0x1d,0x9,0x5d,0x12,0,0]
s=''
s2=[]
for x in range(0,14):
    s+=chr(x ^ a1[x])
print(s)
s+=chr(a2[0])
s2.append(a2[0])
for  x in range(1,14):
    s+=chr(a1[x]^a2[x]^a1[x-1])
    s2.append(a1[x]^a2[x]^a1[x-1])
print(s2)
s+=chr(a3[0]^a2[0])
for x in range(0,13):
    s+=chr(x^(a3[x+1]^s2[x]))

print(s)
```

```
PS C:\Users\86159\Desktop>  & 'C:\Users\86159\AppData\Local\Program
thon-2022.2.1924087327\pythonFiles\lib\python\debugpy\launcher' '61
flag{2378b077-
[55, 100, 54, 101, 45, 52, 53, 54, 52, 45, 98, 100, 99, 97]
flag{2378b077-7d6e-4564-bdca-7eec8eede9a2}
PS C:\Users\86159\Desktop>
```

得到flag为 flag{2378b077-7d6e-4564-bdca-7eec8eede9a2}

总结：本题的难点主要在于OD脱壳