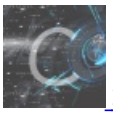
攻防世界 crackme

原创

__N4c1__ 于 2019-08-17 09:07:27 发布 360 收藏

分类专栏： 攻防世界

本文链接：https://blog.csdn.net/qq_43504939/article/details/99688783



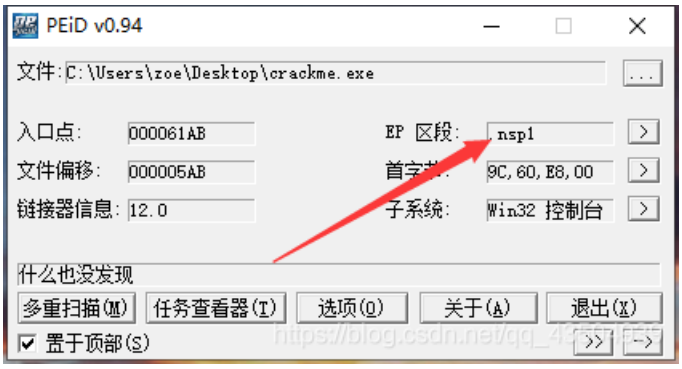
很好的一道题，

还能练习了一把在IDA中使用python脚本，不错，IDA很强大。

预备知识：

- ESP定律
  esp简单介绍

先查壳



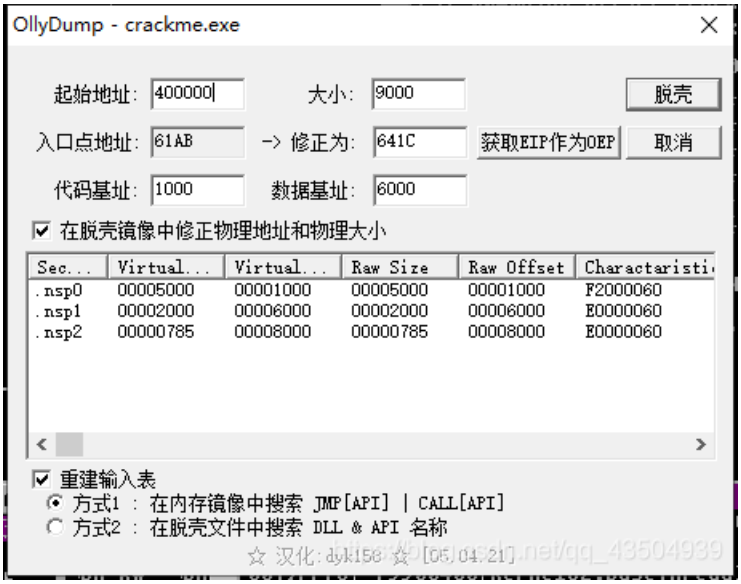
听说是北斗的壳。

用ESP定律脱壳，

这个太简单了，在call处的ESp在数据窗口中跟随，下个硬件断点，

就到了OEP处，

用简单的ODdump脱壳就行了。



载入IDA，无脑f5，

```
4  int v1; // eax
5  char Buf; // [esp+4h] [ebp-38h]
6  char Dst; // [esp+5h] [ebp-37h]
7
8  Buf = 0;
9  memset(&Dst, 0, 0x31u);
0  printf("Please Input Flag:");
1  gets_s(&Buf, 0x2Cu);
2  if ( strlen(&Buf) == 42 )
3  {
4    v1 = 0;
5    while ( (*(&Buf + v1) ^ byte_402130[v1 % 16]) == dword_402150[v1] )
6    {
7      if ( ++v1 >= 42 )
8      {
9        printf("right!\n");
0        goto LABEL_8;
1      }
2    }
3    printf("error!\n");
4LABEL_8:
5    result = 0;
6  }
7  else
8  {
9    printf("error!\n");
0    result = -1;
1  }
2  return result;
3}
```


00001000 sub_401000:24 (4010AA)

简单的异或，

那么就来练习一波学习到的IDA中用python，

这样提取数据就更方便了！

```
from ida_bytes import get_bytes
s = ''
data = get_bytes(0x402130, 0x402140-0x402130)
r = get_bytes(0x402150, 0x402200-0x402150)
print(len(r))
for i in range(int((len(r))/4)):
    s += chr(ord(data[i % 16]) ^ ord(r[i * 4]))
print(s)
```