

# 之前的逆向（6）第三届上海大学生网络竞赛-easy crack

原创

Startr4ck 于 2018-04-28 07:09:28 发布 186 收藏

分类专栏: [ctf](#) 文章标签: [writeup](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 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/shakeyin1998/article/details/80115381>

版权



[ctf 专栏收录该内容](#)

17 篇文章 0 订阅

订阅专栏

## 【题目链接】

<https://www.ichunqiu.com/battalion?t=1&r=59857>

## 【解题流程和思路】

因为分数比较低, 以为直接就能够明文对比, 没想到和想象的不一样, 这道题涉及到Nspack脱壳还有算法破解。

第一步 破解Nspack 壳, 使用 peid 查看发现是 nspack 的3.x 壳。

使用 ESP 定律进行脱壳

第二步 使用IDA对算法进行破解, 使用 F5转换成c 语言之后, 分析算法, 写出对应的解密脚本就可以得到flag

IDA算法

```
1 l1 = "this_is_my_flag"
2 l2 = [0x12, 0x4, 0x8, 0x14, 0x24, 0x3C, 0x4A, 0x3D, 0x56, 0x0A, 0x10, 0x67, 0x0, 0x41, 0x0, 0x1, 0x46, 0x5b, 0x44, 0x41, 0x68, 0x0C, 0x44, 0x72, 0x0C, 0x0D, 0x40, 0x38, 0x48, 0x5F, 0x2, 0x1,
3 f = ""
4 for i in range(len(l2)):
5     f += chr(ord(l1[(sum(l2))%len(l1)]*10**i))
6     print(f)
```

```
opsp
C:\Users\ Administrator\AppData\Local\Programs\Python\Python36\python.exe C:/osk/opsp.py
this_is_my_flag
Process finished with exit code 0
```

得到flag。