CTF挑战赛-合天网安实验室-Reverse逆向200writeup

转载

iqiqiya 于 2018-10-06 16:38:18 发布 1035 收藏
分类专栏： 我的逆向之路 我的CTF之路 ------合天CTF 我的CTF进阶之路 文章标签： CTF挑战赛-合天网安实验室-Reverse逆向200wri CTF挑战赛-合天网安实验室 逆向200writeup


我的逆向之路 同时被 3 个专栏收录
108 篇文章 10 订阅
订阅专栏


我的CTF之路
92 篇文章 5 订阅
订阅专栏


------合天CTF
3 篇文章 0 订阅
订阅专栏

自己做的时候 那个INT3断点一直搞不定 后来按照这篇文章的方法成功

转载自合天小逆向探究断点异常 作者iFurySt

东搞西搞都在瞎搞，今天到合天上面看到一个逆向题(RE200)，拿下来搞了一下，学到了点东西，分享一下。

首先当然是运行一下摸摸套路，接着查了一下无壳，之后就是丢进OD开始调试。

可以根据运行看的字符串找个大概位置，往上翻找到函数入口：

调试一下就到这边了，往下走，password1简单，就是简单的对比字符，直接拿到：

接着看关键的password2，进入函数，跑一下程序死掉了，发现里面有INT3中断，INT3是怎么回事呢，正常运行的时候INT3会交给系统的SEH（异常处理）进行处理，而在调试的时候，中断会交给调试器，之后就会异常退出（若想了解更多请移步google，网上资料很多，不赘述）。

这时候我们打开OD的Debugging options，选上INT3 breaks，因为之前代码有加载SEH，所以会自动交给SEH处理，处理完再返回函数接着执行。

重新调试发现程序还是跑到结束，没办法调试，因为我们不知道SEH结束后返回的地址，查看上面加载SEH的代码可以发现返回的地址40157F，

但是过去看了一下一堆乱码，此时我们打开IDA看一下，真正关键代码是401547（IDA这边已经能看到算法了），我们下个断点，调试一下就知道原始字符串了，再拿出来与2异或一下就得到结果了：

```
s='75316E6E66326C67'
result=''
for i in range(0,len(s),2):
    result+=chr(int(s[i:i+2],16)^2)
print(result)
```

> 在《逆向工程核心原理》里面有一句话：
>
> 有时，在某些环境（OS，调试器插件Bug等）中使用StepInto(F7)或StepOver(F8)命令跟踪INT3指令会导致调试器非正常终> 止。当遇到这种情况时，请按照以上说明设置好断点后再按F9运行程序。

我就是这样的，就是到SEH里不能再F7或者F8的，必须先找到SEH结束后返回的地址，在那之后下断点F9。