XCTF simple-check-100

原创

*^˘^* 于 2020-12-21 16:39:41 发布 75 收藏

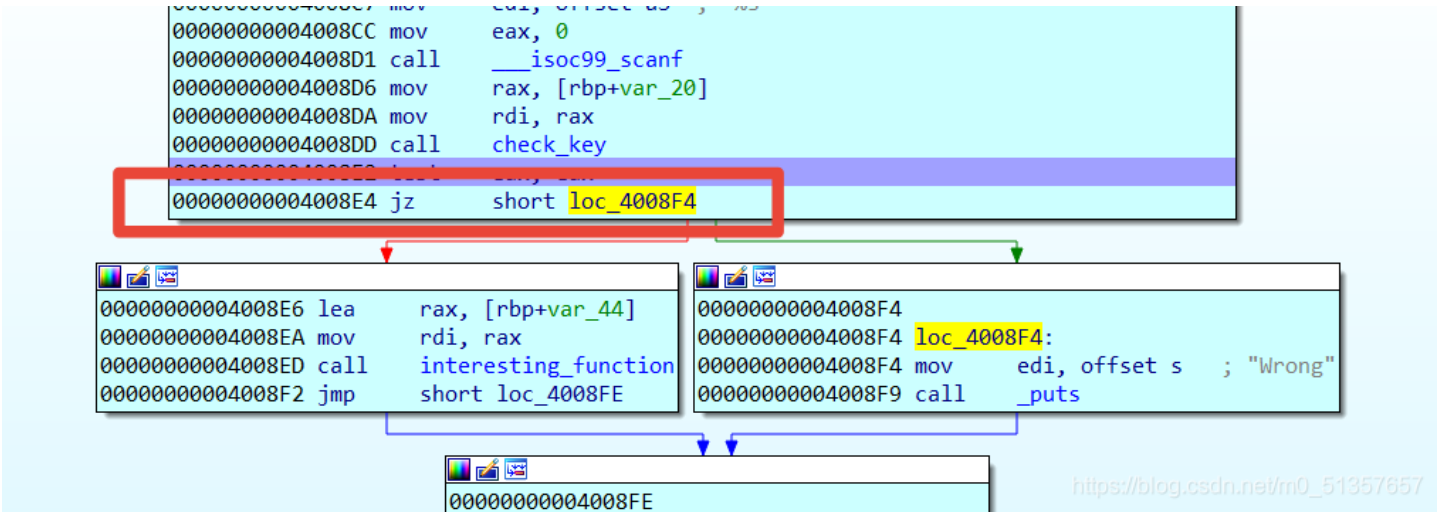
分类专栏： 笔记

本文链接：https://blog.csdn.net/m0_51357657/article/details/111477327

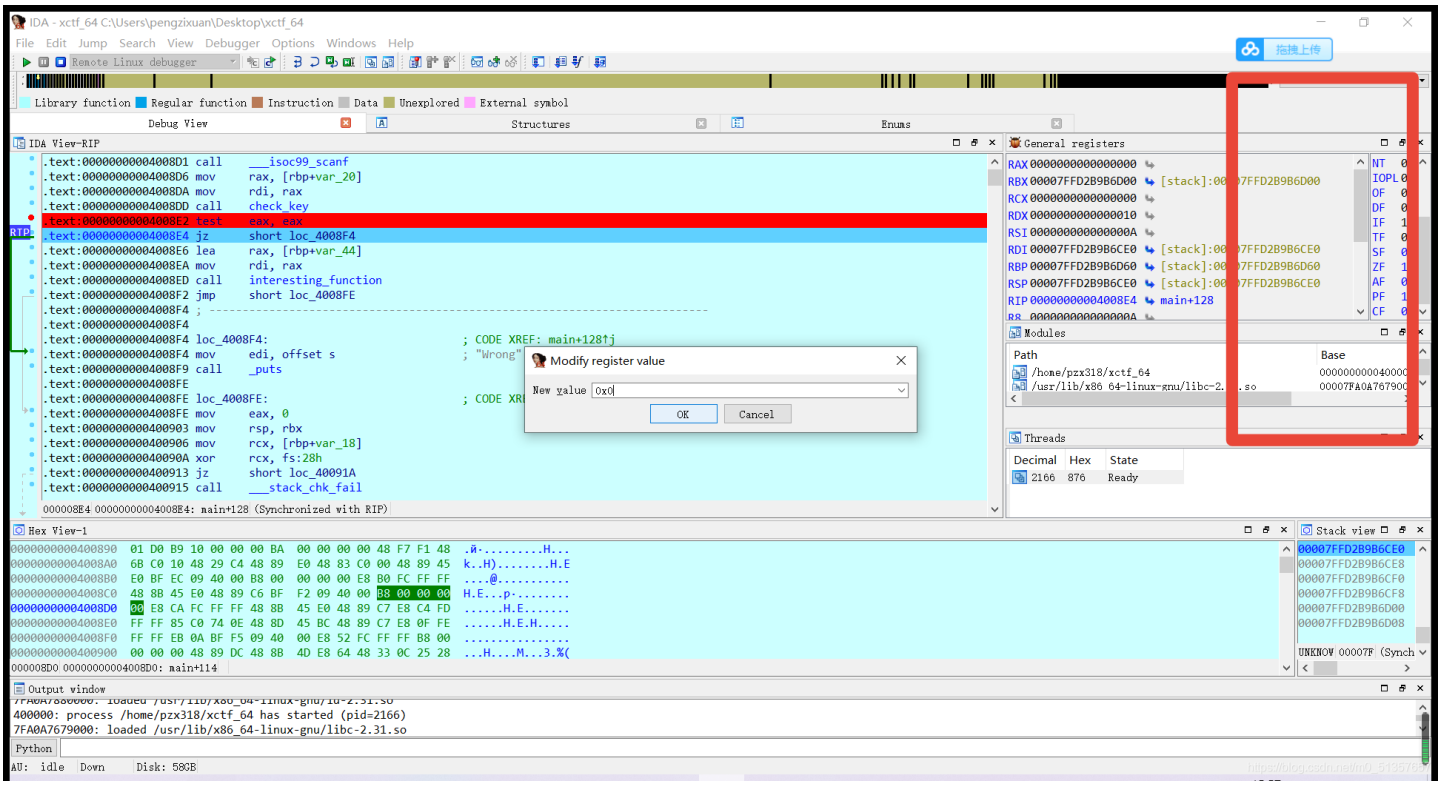
最近在学动态调试，离开了学长指导的废物正式进入龟速学习模式（学长们都太忙了呜呜呜。。。）

题目： XCTF simple-check-100

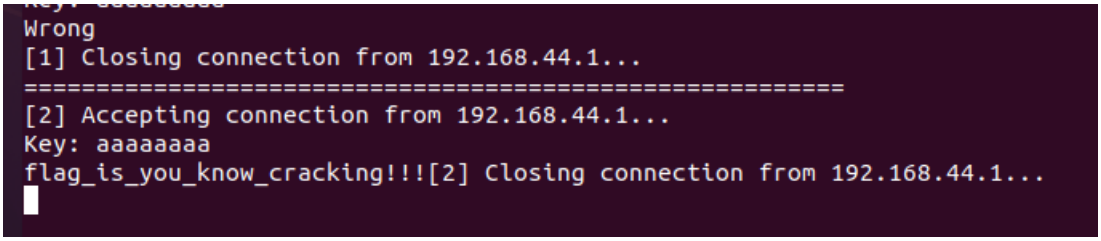
先用ida调试（linux远程调试上一篇学习日记里提到了）



先看一眼逻辑，这道题蛮友好的，关键只有这一个跳转，跳转成功即输出"Wrong!"，跳转失败才能得到flag，那就在跳转的位置下个断点吧。。



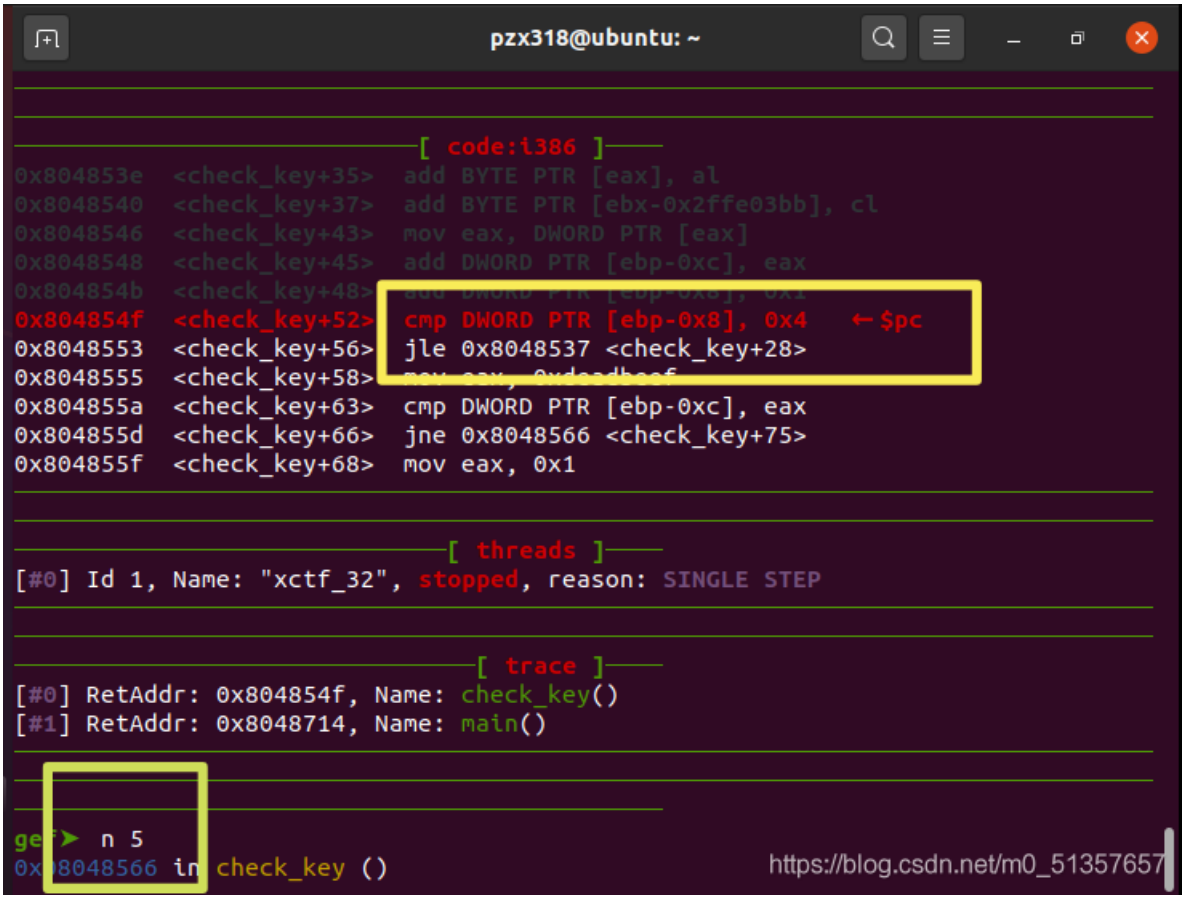
jz指令跳转的条件是Z标志位为1，所以在这里手动改为零



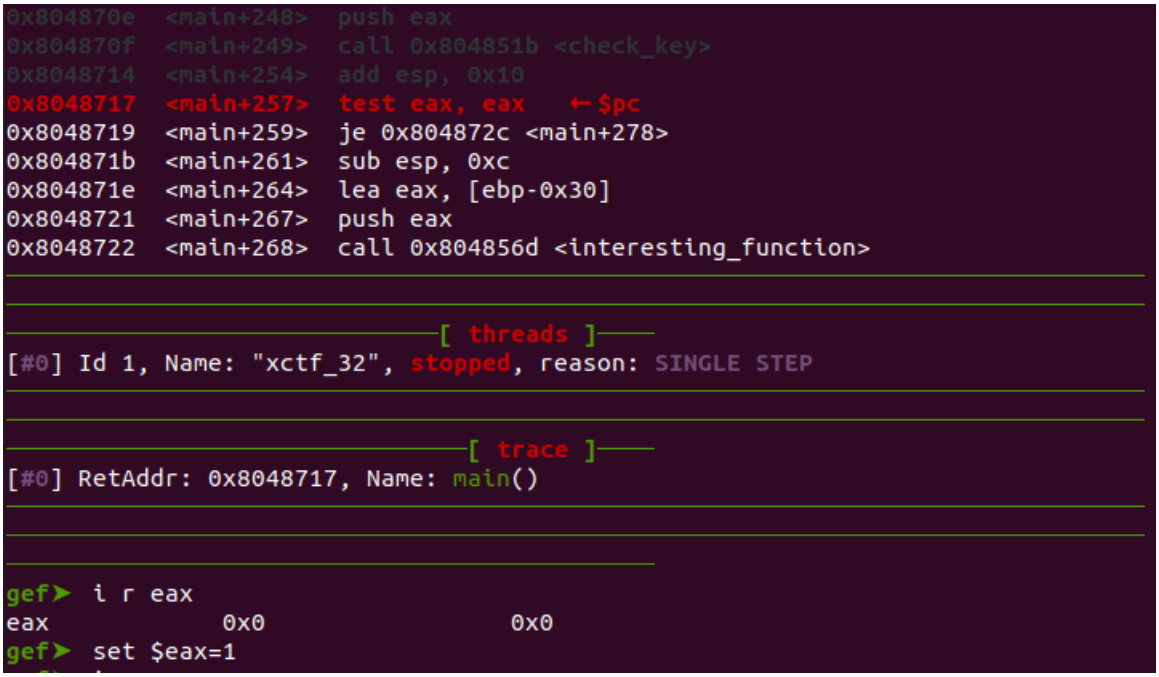
继续运行即可得到flag~

emmm对于windows下调试为什么调不出来我也不太清楚。。。

又跟着别的大佬的wp试了试GDB调试,因为与前面不同，是在check-key之前下的断点，在check-key函数中遇到了一点问题，一直n步入时突然发现一直在回跳，，，



仔细看发现是这里的跳转在搞事情。。直接走五步把这个绕过去。



```
gef➤  i r eax
eax            0x1                 0x1
gef➤  c
Continuing.
flag_is_you_know_cracking!!![Inferior 1 (process 3279) exited normally]
gef➤
```


emmmm虽然学的也不多还是记录一下吧。