babystack

发表于 2021-01-21 分类于 Challenge， 2017， HCTF， Bin
Challenge | 2017 | HCTF | Bin | babystack

点击此处获得更好的阅读体验

WriteUp 来源

https://xz.aliyun.com/t/1589

题目考点

- *栈溢出*
- *ROP*
- *侧信道攻击*

解题思路

这题的名字叫babystack，程序中是一个直接的栈溢出。而且还自带一次任意地址读。 当然这题的难点也很简单，只有read，write，open，exit系统调用。之所以搞出这个题目是受defcon的mute那题的启发。mute那题是用shellcode来实现的侧信道攻击。所以我就想能否用rop来实现侧信道的攻击。

下面是我在libc里找到的一个可以用来侧信道攻击的ROP

```
1 .text:00000000000D72CE                cmp     cl, [rsi]
2 .text:00000000000D72D0                jz      short loc_D7266
3 .text:00000000000D72D2                pop     rbx
4 .text:00000000000D72D3                retn
```

在ret之后用一个read函数来block住代码。而比较成功之后则直接crash退出。使用这种方法来逐字节的比较flag。

当然，解法不止这一种。libc里还有很多种的rop可以用来进行侧信道攻击。可以看看选手们的解法.

poc见github

Flag

```
1 无
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2017/HCTF/Bin/d54KjxkA2oDbxC5fSYKEiS.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # 2017 # HCTF # Bin
ar_u_ok
ippatsu-nyuukon