rroopp

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

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

解题思路

之所以写这个题目，只有一次在写实际栈溢出利用的时候碰到了这个情况。栈溢出是在链接库中，没有打开的可以leak用的文件描述符。而主程序就只有这么一点点代码。当时自己写rop的时候感觉挺有意思的，就拿出来写了这样一个题目(主程序是我直接patch当初那个程序来的，没有源码。可以猜猜是什么程序：)

当然launch.so就是我自己写的程序了。里面大致模拟了ipv4包解析的过程。当然也是一个直接的栈溢出。在最后合并包的时候并没有检查长度而是使用了一个固定长度的栈缓冲区。

当然虽然binary比较小，其实还是有挺多可以用的gadget的。这里还有一个很好玩的技巧，就是dlsym的handle可以指定为RTLD_DEFAULT和RTLD_NEXT来从已经加载的动态链接库中查找函数。所以无需指定handle的值可以可以调用libc中的函数的。

Flag

```
1 无
```

- *本文作者：* CTFHub
- *本文链接：* https://writeup.ctfhub.com/Challenge/2017/HCTF/Bin/quzeM6rroHnUrfFBYxsMZg.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
babyre
old driver