writeup-woo

原创

charlie_heng 于 2016-12-11 09:32:13 发布 179 收藏

分类专栏： 二进制-逆向工程

本文链接：https://blog.csdn.net/charlie_heng/article/details/53571689

题目如下

My friend let me play this sick game. Can you get the hidden flag?

Challenge hosted at: 104.196.15.126:15050

附件下载

把附件下载下来，首先扔进IDA，查了一遍，发现有一个函数pwnme和另外一个函数是用来读文件的，在菜单输入数字4919就可以进入pwnme函数。

扔进linux，用gdb试了一下，发现在生成动物输入名字存放的内存空间就是pwnme读取的内存空间，第一关是要从rax+0x14这个内存地址读取一个值，然后和0x3比较，如果不相同就退出，第二关是从rax中读取一个地址，然后call这个地址，有了思路就很容易解决了

构造payload如下

```
python -c "print '1'+'\n'+'1'+'\n'+'\xDD\x08\x40\x00\x00\x00\x00\x00'+'\x00'*12+'\x03'+'\n'+'4919'+'\n'
```