2019全国大学生信息安全竞赛初赛pwn前四题writeup—栈部分

转载

weixin_33736649 于 2019-04-28 01:09:00 发布 308 收藏
原文链接：http://www.cnblogs.com/ctf-pwn-player/p/10781350.html
版权
ret to libc技巧：https://blog.csdn.net/zh_explorer/article/details/80306965

如何leak出libc地址：基地址+函数在libc中的偏移地址=函数真实地址

1.已知libc，函数地址-函数在libc中的地址=基地址

2.不知道libc，就要leak出libc中的两个函数

转载于:https://www.cnblogs.com/ctf-pwn-player/p/10781350.html