感想

这一次的题目和attack的差不多，所以做的比较快
主要收获有3个吧：
一个是学会了“nop雪橇”的技术，是用来客服站随机化的，emm但是感觉就功能而已应该比rop链弱一点，rop不仅克服站随机化的弱点，还克服了栈不可执行的问题。但是nop雪橇使用起来是比rop更方便的，rop链要找到可行代码挺考验眼力的emm
另一个是理解了缓冲区溢出，原来栈溢出和堆溢出都是缓冲区溢出的一种
最后一个是对调试和汇编和栈都有了更深的理解和熟练度。

因为之前做了attack_lab，相信做buffer_lab会快很多，这里就直接解释最后一关吧

level4

level4有如下要点：
1.要用nop来填充空闲块，以保证即使不直接返回到我们填充的代码，也能顺着nop指令执行到代码
2.一共要填528字节
3.因为栈会偏移正负240，在覆盖testn的返回指令时需要考虑到跳转一定要跳转到某个nop之中，这里直接取折中法，直接选取256字节（主要是直接减0x100比较好算地址），最好把代码放到栈的底部
4.testn的ebp=esp+0x28（可以通过看代码得到）