linux 堆溢出 pwn 指南,[原创]看雪.京东 2018CTF 第六题 PWN-noheap的完全堆溢出解法...

转载

江南憔悴客 于 2021-05-16 08:51:18 发布 55 收藏
文章标签： linux 堆溢出 pwn 指南

今天吃饭的时候看了下公众号推送的解析，里面出题人说道

全题只能leak一次，然后就会关闭输出。这是为了屏蔽有可能的堆利用方法。

觉得有些不对劲，因为输出关闭并不影响堆利用啊，leak完了继续打就是了，只不过没有回显。

然后睡午觉时忽然想起还是可以走house of orange的。

当时我觉得堆和bss同时溢出比较麻烦，很容易覆盖到vmcode，造fake file可能会有麻烦，所以放弃了house of orange。

但今天一想感觉偏移0x70的几个成员变量似乎不是很重要，不影响利用。尝试走了一下，发现几个和利用有关的变量仍然可以控制，所以还是可以的。

总体思路就是先造leak，然后走size-1的溢出去盲着覆盖Unsorted bin，注意覆盖时在vmcode对应偏移处复制一份原来的16个byte，整体还是常规的house of orange。

于是造出来的fake file如下所示。

$13 = {

file = {

_flags = 0x0,

_IO_read_ptr = 0x61,

_IO_read_end = 0x7ffff7dd1bc8,

_IO_read_base = 0x7ffff7dd1bc8,

_IO_write_base = 0x0,

_IO_write_ptr = 0x1,

_IO_write_end = 0x0,

_IO_buf_base = 0x7ffff7b99d57,

_IO_buf_end = 0x0,

_IO_save_base = 0x0,

_IO_backup_base = 0x0,

_IO_save_end = 0x0,

_markers = 0x0,

_chain = 0x0,

_fileno = 0x1130301,

_flags2 = 0x106040f,

_old_offset = 0x4000161302011409,

_cur_column = 0x0,

_vtable_offset = 0x0,

_shortbuf = {0x0},

_lock = 0x0,

_offset = 0x0,

_codecvt = 0x0,

_wide_data = 0x0,

_freeres_list = 0x0,

_freeres_buf = 0x0,

__pad5 = 0x0,

_mode = 0x0,

_unused2 = {0x0 }

},

vtable = 0x7ffff7dd0798

}

可以看到vmcode落在了伪造出的fake file的_fileno _flags2 _old_offset几个成员上，对利用流程没有影响。

故此题可以完全无视那个vm，走house of orange的套路完成攻击。

感慨自己真是越来越迟钝了，比赛时这么简单的方法都没想到，跑去逆vm干啥……真是越活越倒退了。

最后于 2018-6-29 17:19

被diycode编辑

，原因：