Pwntools的学习笔记

from pwn import \* 将所以的子模块和一些常用的系统库导入到当前的空间。

sh = process('./XXX ') 其中XXX为ELF文件，为Linux下面的可执行文件，process为本地链接文件。

sh.sendline(payload) 把构造好的payload输入到sh所指向的文件或者地址+端口里面去,默认在行尾加\n

sh.recvline('XXXXX') 接收一行，可选择是否保留行尾的\n

sh.interactive() 可同时读写管道，相当于回到shell模式进行交互，在取得shell后调用

cyclic 200 生成200个字符，用来查找偏移，来确定返回地址。

p32() 32位ELF程序用的 p64() 64位ELF程序用的