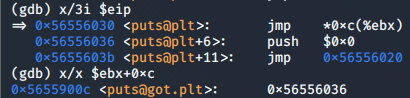
got表和plt表过程（以puts为例）：

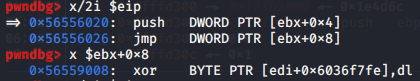
调用外部库函数puts时，先调用call puts@plt，



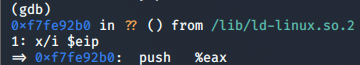
然后跳转到puts@got.plt所指向的地址（此时指向puts@plt第二条指令），



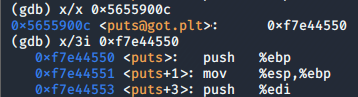
然后跳到.plt节的开头



然后通过jmp最终跳转到ld-linux.so.2解释器，



解释执行完毕后，解释器将把puts@got.plt的旧值改变为puts函数地址。



ret2plt攻击时，可以修改puts@got.plt的内存为恶意地址。