C(pp)通过指针（new）访问堆中元素，malloc…（返回的指针在栈上/寄存器中）

访问全局变量：lea Imm(%rip)

访问临时变量：lea Imm(%rsp/%rbp)

便于ASLR，核心是保持内部相对位置不变

阴影的地方：什么也没有，表示空指针

ASLR两种：Text下方，Stack前后

canary最后一位一定为0

一个程序的所有函数的金丝雀值都是一样的