P198-203

- 如何对抗缓冲区溢出攻击
  - 栈随机化，使得栈位置不容易被预测，让攻击者更加困难。
    - 策略：程序开始分配内存时，在栈上先分配 0-n 字节的随机大小空间；
    - linux 中的标准行为，也叫做地址空间布局随机化
  - 栈破坏检测
    - 很好地防止了溢出攻击破坏存储在程序栈上的状态，性能损失也很小
  - 限制可执行代码区域
    - 消除攻击者向系统中插入可执行代码的能力，限制哪些区域可以存放可执行代码。
- 变长栈帧

有的函数，局部存储的对象是需要变长的。

需要理解数组和对齐