缓冲区溢出漏洞

缓冲区是指内存空间中用来存储程序运行时临时数据的一片大小有限并且连续的内存区域

1.栈溢出漏洞

1.系统栈

是操作系统在每个进程的虚拟内存空间中为每个线程划分出来的一片存储空间，由系统自动维护，用于实现高级语言中的函数调用，**系统栈从高地址向低地址增长，数组的低位位于低地址**。栈中保持4字节对齐，填充FF

三个重要的寄存器：

- **ESP**：栈指针寄存器，存放当前栈帧的栈顶指针
- **EBP**：基址指针寄存器，存放当前栈帧的栈底指针
- **EIP**：指令寄存器，存放下一条等待执行指令的地址

函数调用过程

1. 参数入栈：被调用函数的参数从右向左一次入栈
2. 返回地址入栈：将call指令的下一条指令的地址入栈
3. 代码区跳转：处理器从代码区的当前位置跳到被调用函数的入口处
4. 栈帧调整：
    a. push ebp 保存调用者的栈底
    b. mov ebp, esp设置新的栈底
    c. sub esp，xxx 开辟栈空间

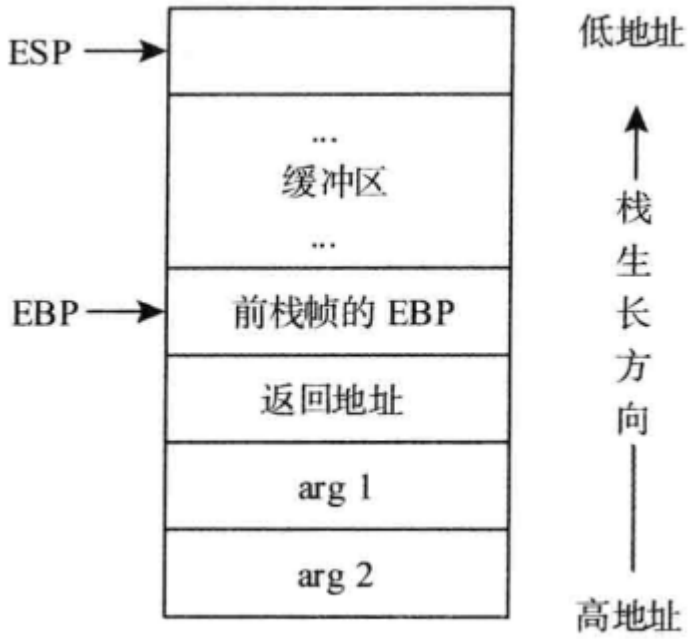

图 4-3　执行函数调用指令后的栈帧状态图

函数返回过程

1. 保存函数返回值： 将函数返回值到eax寄存器中
2. 回收栈空间： add esp, xxx降低栈顶，回收当前的栈帧空间（实现堆栈平衡）
3. 恢复调用者栈帧：pop ebp
4. 返回原指令序列：retn

ROP攻击

就是面向**返回语句**的编程方法

借用多个retq前的一段指令拼凑成一段有效的逻辑，从而达到攻击的目标。