注入

远程线程注入

利用`CreateRemoteThread`在目标进程内创建远程线程启动`LoadLibrary`加载DLL

缺点：在目标进程空间中有注入的DLL

改进

利用`VirtualAllocEx`在目标进程空间中申请空间，将可执行代码写入申请的空间`buf`中。
`CreateRemoteThread`启动`buf`处的代码

调试

1. 正面调试，开两个调试器调试
2. 本进程自己注入自己，可以一个调试器调试
3. 在代码关键处写入`int 3`调试中断，目前XP上可用

地址修正 —— 重定位

涉及：病毒传播、壳

> 一段内存， 求运行时C的地址（C'）
> A ------ C ---------- B 编译期地址
> A' ------ C' ---------- B' 运行时地址
> C' = C + (A' - A)

```
call next   ; 压入了运行地址next的地址 -- 压下条指令地址
next:
    pop ebx ; 获取了运行地址next的地址
    sub ebx, offset next ; 运行地址next - 编译时地址next = 偏移（修正量）
```