注入方法

> **本质**:
>
> > 代码能写到对方进程, 代码有执行机会

1. LoadLibrary,注入DLL

> 通过写远程内存,写入DLL名 ,直接传入LoadLibrary的地址,远程加载DLL

2. 远程线程

> 注入ShellCode 进行注入代码,或者注入代码Load_Dll

3. 虚表注入

> 预先探测虚表项的调用时机与频率, 给予一个Inject的函数质性机会

4. GetThreadContext

> 通过修改该Context,改变线程执行流程, 带起我们的代码

5. API HOOK

> X32 Demo

> X64 Demo

6. 输入法注入

> 伪装一个输入法程序, 切换输入法带起 写入DLL

7. 注册表键值

> 修改COM组件在注册表的路径, 进行COM劫持

8. (修改/加入)PE中的导入库的名称

> 利用PE加载原理, 带起自定义的DLL

9.PE加载器

> 用PE加载器模拟系统, 进行加载目标程序, 让目标程序生活在PE加载器的肚子里

10. Path程序入口点

> 对PE打补丁,修改程序入口点到我们的自定义代码上, 然后流程转移到OEP

---

11. SetWindowsHookEx全局钩子

> 修改指定窗口的过程函数, 为待注入的DLL的导出函数, 则目标程序会自动加载此DLL, 进而进行注入

12.DLL劫持

> **选择战场很重要**, 选择目标DLL 进行导出函数劫持
