DLL远程注入

1. virtualallocex //目标内存申请一段空间
2. Virtualprotect//修改申请内存页读写属性
3. WriteProcessMemory//跨进程写入内存，将dll名写入目标内存
4. CreateRemoteThread//创建远程线程，参数LoaadLibrary地址，目标进程内路径名

5.Waitforsingleobject//等待线程退出

InlineHook

1.保存hook api前5个字节 char API[5] = {0} ;memmove(API,MessageBox,5);

2.JmpOpcode[5] = {E9};*(DWORD*)(JmpOpcode + 1) = (DWORD)MessageBox - (DWORD)pfun - 5;

3.Memmove(MessageBox,JmpOpcode,5)//将JmpOpcode拷贝到MessageBox前5个字节