[网络安全自学篇] 八十五.《Windows黑客编程技术详解》之注入技术详解（全局钩子、远线程钩子、突破Session 0注入、APC注入）

原创

Eastmount 于 2020-06-25 20:04:44 发布 16019 收藏 140

分类专栏： 网络安全自学篇 文章标签： 系统安全 Windows黑客编程 注入技术 APC注入 远线程钩子

从这篇文章开始，作者将带着大家来学习《Windows黑客编程技术详解》，其作者是甘迪文老师，推荐大家购买来学习。作者将采用实际编程和图文结合的方式进行分享，并且会进一步补充知识点，希望对您有所帮助。第二篇文章主要介绍4种常见的注入技术，包括全局钩子、远线程钩子、突破SESSION 0隔离的远线程注入、APC注入，案例包括键盘钩子、计算器远线程注入实现、APC注入等，希望对您有所帮助。

为了方便对目标进程空间数据进行修改，或者戴上目标进程的“面具”进行伪装，病毒木马需要将执行的Shellcode或者DLL注入到目标进程中去执行，其中DLL注入最为普遍。

这是因为DLL不需要像Shellcode那样要获取kernel32.dll加载基址并根据导出表获取导出函数地址。若DLL成功注入，则表示DLL已成功加载到目标进程空间中，其导入表、导出表、重定位表等均已加载和修改完毕，DLL中的代码可以正常执行。正是由于DLL的简单易用，才使得DLL注入成为病毒木马的常用注入技术。

- **全局钩子：** 利用全局钩子的机制
- **远线程钩子：** 利用CreateRemoteThread 和 LoadLibrary函数参数的相似性
- **突破SESSION 0隔离的远线程注入：** 利用ZwCreateThreadEx函数的底层性
- **APC注入：** 利用APC的机制

文章目录