[网络安全自学篇] 九十四.《Windows黑客编程技术详解》之提权技术（令牌权限提升和Bypass UAC）

原创

Eastmount 于 2020-09-12 21:43:21 发布 16592 收藏 405

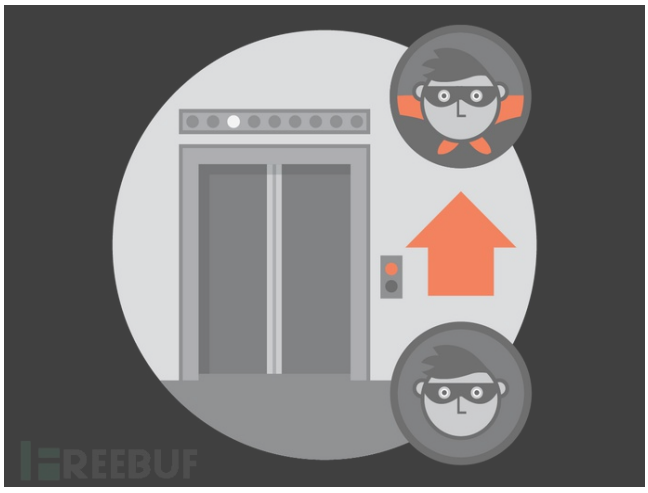
分类专栏： 网络安全自学篇 文章标签： Windows黑客编程 提权技术 Bypass UAC 进程提权 网络攻防

本文链接：https://blog.csdn.net/Eastmount/article/details/108486283

这是作者网络安全自学教程系列，主要是关于安全工具和实践操作的在线笔记，特分享出来与博友们学习，希望您喜欢，一起进步。这篇文章将带着大家来学习《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，并且会进一步补充相关知识点。第六篇文章主要介绍木马病毒提权技术，包括进程访问令牌权限提升和Bypass UAC，希望对您有所帮助。

如果把权限看作是门禁卡，那么计算机便是一栋拥有许多门禁的大楼，要想进入一个房间或办公室，则需要拥有对应房间的门禁卡。对于低权限，即拥有很少数量的门禁卡，能去的也只有厕所之类的无关紧要的地方，无法进入层层设防的保密办公室。这样，即使病毒木马成功混入计算机这所大楼，如果没有足够的权限，也不能窃取或修改计算机中的关键数据，杀伤力有限。

因此，提权技术（从低权限获取高权限的技术）成为大多数病毒木马必备技术。



计算机上有哪些操作需要提权呢？操作系统处于安全考虑，对不同的操作系统划分了权限。例如创建或修改系统服务、修改HKEY_LOCAL_MACHINE注册表键或重启移动文件等操作，均需要管理员权限，普通权限操作会失败。

同时，从VISTA系统引入了UAC（用户账户控制），涉及权限操作时都会有弹窗提示，只有用户点击确认后，方可继续操作。所以，VISTA之后的提权操作主要是针对UAC不弹窗静默提权