**Windows 系统开发人员必备知识**

最后更新：2020/6/01

拟定：高冲

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | 基本 | 进阶 |
| 1 | 工具使用 | SysinternalsSuite  procexp.exe 、Procmon.exe | 其他工具及系统自带工具  dirquota.exe / cacls.exe / secedit.exe |
| 2 | 文件管理 | 文件的创建、修改、删除  文件的遍历，查找 | NTFS 权限，设置目录共享，ACL；（先熟悉用户管理章）目录监视、文件保护 |
| 3 | 进程管理 | 进程创建、结束、查找  获得进程ID ，句柄，路径…. | 进程详细信息，父进程、子进程、进程资源消耗、进程优先级…  进程提权、UAC 保护、进程监视 |
| 4 | 系统服务 | 自己写一个系统服务程序。  控制整个生命周期：创建、停止、运行中、卸载 | 控制其他人的服务；停止和启动别人程序的服务。 |
| 5 | 用户管理 | Windows 的系统帐号管理，用户|用户组 的创建、删除、修改；  用户加入用户组，用户移出用户组。 | 用户配置中各个参数的设置。 |
| 6 | 注册表|组策略 | 注册表分析与查找，注册表各种类型数据的读取与写入。 | 安全策略设置，组策略设置 |
| 7 | WMI | VC 调用 WMI ，系统信息查询 |  |
| 8 | Windows COM  组件 | VC 调用Windows系统COM 组件来实现操作系统的功能 | 桌面管理、窗口管理 |
| 9 | DLL | 封装自己DLL 调用第三方的DLL |  |
| 10 | HOOK | 应用层Windows API 钩子、  消息钩子 的拦载回调处理 | 驱动级的实现 |
| 11 | WTS 相关函数 | Windows Terminal Services 相关的函数，远程用户会话管理，用户监视、断开、注销 | 用户会话下的进程管理 |
| 12 | 防火墙  计划任务  系统日志  … | VC 调用系统API 或 COM 实现对防火墙、计划任务、系统日志…  的调用 | 其他更多 MMC 控制台组件的调用 |