破解的时候多在系统函数中下断，分析逆向

Ntapi

Ntdll的api

程序错误处理 函数失败时返回值类型 bool 句柄或Null pvoid long

检测到错误会调用本地 线程存储TLS 错误代码号 getlasterror（错误代码号）

线程最后的错误代码 formatmessage作用很多 可以编码错误代码

2、定义错误代码

二、unicode 1、单字节和双字节 2、unicode函数 W 枚举资源 输出文字

3、窗口创建4、字符串函数 5、资源 6、字符串转换

1. 内核对象

创建 打开 操作 符号对象 事件 文件 文件映射 io 作业 互斥 管道 进程 信标 线程 计时器 对象的数据只能在内核访问，外面只能调用api接口

对象句柄 对象属于内核 而不属于进程，利用使用计数来撤销对象 安全描述符 对象的使用者（服务器中用） 可以自己编辑描述符

2、进程内核句柄表 一个数组包含对象指针 访问屏蔽和标志

创建内核对象 文件 线程 文件映射 创建错误可能返回0也可能返回-1，要注意

关闭内核对象 closeHandle 3、内核对象共享 文件映射 邮箱 管道 互斥同步

(1)父子进程继承 可继承句柄声明CreateProcess 传入继承参数 改变句柄的继承标志SetHandleInformation(2)命名对象 create时输入名字 可以用继承性或者duplicateHandle对象句柄复制 （3）Open函数带上名字

Getlasterr 名字空间

四、进程 管理进程的内核对象+进程地址空间 数据+代码+dll+堆栈+堆 线程时间片

1、 cui 和gui的连接不同 入口点winmian 或者main wWinmain

启动函数 检索命令行 环境变量 全局变量初始化 初始化栈和堆 调用构造函数

getStartupInfo() winmain() 2、进程实例句柄 winmain第一参

getmoudlehandle() 返回模块（）或者dll的内存地址

亲缘性 错误模式:如何处理错误 setErrorMode() 驱动器目录 当前目录 系统版本

3、创建进程 4、startupinfo 包含大量窗口信息

线程池

硬件异常 软件异常