APIHOOK 基址 ce模块基址+偏移 双击地址，数据结构可能保存在一起

HOOK拦截消息 线程钩子 系统钩子 安装钩子 卸载钩子 拦截对API函数的调用

键盘钩子 鼠标钩子

全局钩子

钩子类型 发送到窗口过程的消息

钩子回调函数 下一个钩子函数 钩子类型 函数地址 所在实例句柄

这些函数写成dll 然后主程序注入代码 ，调用dll函数 一般是hook到原系统dll函数入口 需要保存原地址 然后 jmp 用读写内存来改写代码

一、字节序:针对大小超出一字节的数据 不包括数组等 windows上是小端

字符集 Unicode

2、Win32api 子系统到核心层 使用dll 显式调用 隐式连接（在创建的时候lib连接）

子系统 kernel user gdi

常用 获取窗口文字 获取对话框句柄 getdlgitem getdlgitemtext获取对话框文字 获取对话框数值 显示消息框

句柄：标识各种东西 如进程，文件，设备，菜单 进程句柄表

消息机制 应用消息队列 系统消息队列 先到系统 然后传给应用

发送消息 wm\_command 一般是选择控件时发送 \_destory \_quit \_gettext拷贝到缓冲

保护模式 16位 32eax 64位rax 段寄存器 fs gs 实模式 dos 保护模式windows

虚拟内存 ds:[] 段选择器放的是段选择子 不寻址 只是全局描述符表 和本地描述符表GDT LDT的指针

平坦模式 4G虚拟空间 用的是映射方式 操作系统全程映射 应用代码只在自己的时间映射? 数据 dll会被映射到进程的空间内

应用权限 ring0 ring3

3、wow64

二、动态分析 调试器 常用断点 插件 run trace hit trace

X64dbg mdebug windbg

内存 线程 CPU（寄存器 ） 堆栈 数据（内存直接数据）反汇编（内存解释出代码） 信息

单步 跳过call 跳到ret 返回程序领空

断点

三、静态分析 文件类型分析

2、反汇编引擎 beanEngine Udis86 CAPSTONE ASMJit

KeyStone

静态反汇编 IDA

十六进制工具

四、逆向分析技术 汇编代码分析

五、演示版保护 序列号 注册机 警告窗口 时间限制 菜单功能限制 keyFile

网络验证 光盘检测 禁止多开 断点设置技巧

六、加密算法 散列md5 sha sm3 对称加密 rc4 tea idea blowfish aes sm4

公开密钥算法 ras dsa 椭圆曲线 sm2

其他算法 ctc32 base64

常见加密库

七、系统 内核基础

权限级别 内存空间布局 windows启动过程

R3与r0通信

内核函数

驱动模块

内核的重要数据结构

内核对象

Ssdt teb peb

内核调试 winbdg双机调试 查看ssdt shadow ssdt

八、异常处理 异常列表 处理过程

Seh 数据结构 处理程序注册和卸载 异常分发的过程 线程异常处理 栈展开 顶层

X64 异常分发 wow64

Seh进行验证输入 seh加密解密应用 veh api hook

九、调试api 函数 事件 创建进程并跟踪 循环体 调试事件的处理程序 线程环境 代码注入

十、VT技术 硬件虚拟化 结构 汇编指令 EPT 检测VT支持 VMCS配置 开启

内存隐藏 VT调试

十一、PE格式 基地址 载入的地址 虚拟地址 内存地址 相对虚拟 pe中写的地址 文件偏移 dll需要重定位

入口点 执行的第一行代码 （一般指启动函数，调试器一般会断在main函数）

段选择子 cs:va

DOS头 PE头 字段 结构

十二、注入技术

1. DLL 注入

十三、Hook技术

Api hook

IAT HOOk inline HOOk

分类 address hook inlinehook 基于异常处理的hook

Hook位置选择

Hook 实施过程 address hook inline 异常

二次hook

Detour

检测恢复对抗

十四、漏洞分析技术

漏洞原理 溢出 UAF ShellCode

漏洞利用

十五、壳 各种壳介绍

十六、脱壳 加载过程 脱壳机 手动脱壳

1、寻找OEP 跨段指令 内存访问断点 栈平衡 编译语言特点

1. DUMP 原理 反DUMP
2. 重建输入表 IAT地址 和大小 import REC 输入表加密
3. DLL 脱壳 OEP dump 输入表 重定位表 附加
4. 数据

十七、防范 防算法求逆 抵御静态分析 花 smc 信息隐藏 多态变形

2、文件完整性校验 crc 校验和 内存校验

3、代码和数据结合

十八、 反跟踪

Beingdebugged ntglobalflag heap magic

Native

18.2.1 CheckRemoteDebuggerPresent 677  
18.2.2 ProcessDebugPort 677  
18.2.3 ThreadHideFromDebugger 680  
18.2.4 DebugObject 682  
18.2.5 SystemKernelDebuggerInformation 686  
18.2.6 Native API 688  
18.2.7 Hook和AntiHook 693

调试器检测

防止附加

父进程检测 时间差 trap flag陷阱标志 双进程保护

十九、外壳编写 原程序读取处理 加 外壳用汇编写?或者用c++ 加载过程 添加到原程序

二十、虚拟机设计

二十一、VMP逆向和还原

二十二、补丁技术

文件补丁

内存补丁 技术:跨进程内存存取（create） debugapi 调试寄存器机制 dll注入

Hook vt技术

Smc补丁

补丁工具

二十三、代码二次开发 进行大量修改

数据对齐 增加空间 间隙 手工构造区块 工具

调用函数 输入函数 调用dll

重定位 重定位表修复 自定位

输出函数

消息循环的修改 wndproc

菜单扩展

Dll扩展 接口 消息循环