第一章 进制、寄存器与汇编指令（汇编与C语言相结合）   3000元  
学习汇编能做什么（逆向，游戏安全，加固/脱壳，反病毒，漏洞挖掘等等必备基础）  
1.1   计算机的基本构造及其运行原理  
1.2   不同进制的书写方法  
1.3   为什么计算机要用二进制  
1.4   不同进制间如何运算1  
1.5   不同进制间如何运算2  
1.6   为什么要用十六进制  
1.7   什么是逻辑运算  
1.8   计算机的计数与数学计数的区别  
1.9   谁能告诉我计算机有多少通用寄存器  
1.10  安装VC2012/VC6,写简单的汇编  
1.11  怎么操作汇编指令  
1.12  什么是内存  
1.13  寄存器与内存有什么区别  
1.14  怎么把[ ]里面的值变成地址  
1.15  堆栈的作用。  
1.16  函数的调用过程1  
1.17  函数的调用过程2  
1.18  汇编指令运算过程中，出现进位借位，或者溢出该怎么办  
1.19  对寄存器ESI或者EDI操作的指令有哪些  
1.20  指令和内存有什么联系  
1.21  如何用汇编写程序  
1.22  逆向的起源。什么是内存框架  
1.23  用汇编怎么调用函数  
1.24  不用CALL指令，如何调用函数  
考试：用汇编写一个程序  
  
  
第二章 C语言(软件开发必备)       2500元  
2.1 C语言有哪些规则，如何赋值  
2.2 什么是C语言表达式  
2.3 “如果”代表C语言的哪条语句  
2.4 “如果明天下雨，我不去逛街”该如何用C语言表达  
2.5 假设（a\*4）怎么用移位表达，a向哪边移，移多少  
2.6 C语言有哪些循环语句  
2.7 C语言for 语句该如何使用  
2.8 什么是C语言变量  
2.9 “现在有相同类型的100个变量”，怎么用一条C语句实现  
2.10 什么是二维数组，二维数组跟一维数组有本质上的区别吗  
2.11 C语言结构体是什么  
2.12 怎样合理的运用C语言结构体  
2.13 C语言变参函数有什么作用  
2.14 深刻理解switch 语句1  
2.15 深刻理解switch 语句2  
2.16 C语言宏定义有什么好处  
2.17 什么是C语言指针, 指针是怎么赋值的  
2.18 C语言指针和数组有什么区别  
2.19 C语言指针是有符号的，还是无符号的  
2.20 “void a ;” 这样定义可以吗？什么是空指针  
2.21 指针数组和数组指针分别代表什么  
2.22 指针数组和数组指针的区别在哪里  
2.23 怎样定义C语言函数指针  
2.24 C语言函数指针有什么作用  
2.25 数据结构之单链表  
2.26 数据结构之双链表  
2.27 数据结构之数组  
2.28 数据结构之队列  
2.29 数据结构之二叉树  
项目：学生管理系统或者贪吃蛇小游戏  
  
  
第三章 C++与MFC/逆向练习    3000元  
3.1 结构体与类有什么区别   
3.2 this指针的本质   
3.3 继承有什么好处   
3.4 多态与虚函数有什么联系   
3.5 什么是运算符重载   
3.6 模板是怎么运用的   
3.7 一个Win32程序的执行过程(消息机制的本质)   
3.8 MFC与Win32程序的关系   
3.9 熟记MFC类层次结构   
3.10 控件的使用   
3.11 任意程序窗口句柄遍历   
3.12 逆向窗口程序的通杀方法   
3.13 OD和IDA的基本用法  
3.14 逆向练习（搜集各种C/C++例子进行逆向练习）  
练习：SOFTICE核心文件逆向  
  
  
第四章 汇编编码     3000元  
学习硬编码的好处：(HOOK函数，系统HOOK, 代码变形，VM还原，TMD还原，解释器，调试器必备基础，这就是杀毒软件可以横行的法宝)  
机器码，简称汇编编码，俗称硬编码  
4.0 寄存器 （32位汇编；64位汇编）  
4.01 汇编指令  
4.02 堆栈  
4.03 逆向框架xpose  
4.04 函数内部运行机制  
4.1  定长编码 （0x40-0x4f  0x50-0x5f  0x70-0x7f  0x0f 0x80 – 0x0f 0x8f)  
4.2  定长编码（0x04-0x07  0x0c-0x0f  0x14-0x17  0x1c-0x1d  0x24-0x27  0x2c-0x2d  0x34-0x37  0x3c-0x3d.）  
4.3  定长编码 （0x60 0x61 0x90-0x97 0xa8 0xa9 0xb0-0xbf  0xc2 0xc3 0xcc 0xcd 0xd4 0xd5 0xe0-0xe3 0xe8 0xe90 0xf8-0xfd等等）  
4.4  硬编码4 （写程序把定长编码打印出来）  
4.5  硬编码5 （写程序把定长编码打印出来）  
4.6  变长编码  (0x88 0x89 0x8a 0x8b)  
4.7  变长编码  (0x88 0x89 0x8a 0x8b)  
4.8  变长编码  (0x00-0x03 0x08-0x0b 0x10-0x13 0x18-0x1b 0x20-0x23 0x2b-0x2b 0x30-0x33 0x38-0x3b )  
4.9  变长编码 （0x84-0x87 0x8c-0x8e 等等)  
4.10 写程序把变长编码打印出来  
4.11 写程序把变长编码打印出来  
4.12 写程序把变长编码打印出来  
4.13 前缀 （0x26 0x2e 0x36 0x3e 0x66 0x67 0xf0 0xf2 0xf3)  
4.14 写程序处理前缀  
4.15 写程序处理前缀  
4.16 组编码 (0x80-83  0xc6-0xc7  0xd0-0xd3 等等)  
4.17 写程序处理硬编码  
4.18 0F开头两个字节的编码  
4.19 编写反汇编引擎  
4.20 VMP的核心解释器基本原理  
  
项目：反汇编引擎，解释器框架  
  
  
第五章 Win32 API (只要是项目，都会调用API)    2500元  
5.1 文件操作   
5.2 内存管理   
5.3 进程线程   
5.4 线程同步   
5.5 进程间通信   
5.6 网络通信   
5.7 未公开API的使用   
  
  
第六章 PE     3500元  
学习PE的好处（加密解密，写壳，脱壳，注入，重载操作系统）  
6.1  PE有哪些结构1  
6.2  PE有哪些结构2  
6.3  为什么要有节表，节表有什么好处  
6.4  PE 磁盘拷贝到内存 （写程序）  
6.5  PE 内存拷贝到拷贝磁盘，存盘（写程序）  
6.6  怎么给PE添加一个节  
6.7  PE扩大节有什么好处  
6.8  PE合并节有什么作用  
6.9  PE 输入表 （写程序打印输入表）  
6.10  PE 输入表 （写程序打印输入表）   
6.11  PE 输出表 （写程序打印输出表）  
6.12  PE 输出表 （写程序打印输出表）  
6.13  PE 重定位表   
6.14  修改OEP 弹出MessageBox  
6.15  添加节，拷贝一段函数进去  
6.16  病毒的框架  
6.17  病毒是如何在函数入口植入的  
6.18  病毒是如何写入PE的  
6.19  DLL应用及书写方式  
6.20  UPX壳的源码及其运用  
6.21  加密壳原理和方式  
项目: 手写PE分析工具LoadPe   
  
  
**进阶篇**  
先复习 前面的基础篇的知识，然后写一个解释器完整版（20天）  
  
第七章 保护模式-段寄存器）（2个多月）  5000元  
7.1 段寄存器构成  
7.2 保护模式 GDTR IDTR  
7.3 GDTR,IDTR均为48bit结构体  
7.4 超线程与多核  
7.5 保护模式 获取段寄存器的值  
7.6 保护模式 GDTR.ATTRIBUTES   
7.7 保护模式之修改段寄存器  
7.8 保护模式  调用门  
7.9 保护模式 中断门 陷阱门  
7.10 保护模式 CS:EIP  
7.11 保护模式  RETF,IRETD  
7.12 保护模式  门Dword Count   
7.13 保护模式  任务门  
7.14 保护模式  3环进1环  
7.15 保护模式 10-10-12 分页  
7.16 保护模式 PDT PTE  
7.17 保护模式  页的特点  
7.18 保护模式  TLB  
7.19 保护模式  异常与保护  
7.20 保护模式 2-9-9-12  
7.21 保护模式 CR0~CR4  
7.22       10-10-12和2-9-9-12分页转换  
7.23-7.30 编写CE与内存搜索工具（VT引擎）  
  
  
第八章 操作系统 （2个多月，差不多3个月）   5000元  
本章主要讲解及应用于：驱动保护，系统保护，游戏保护，底层开发，系统架构，架构师，引擎开发等…  
8.1 操作系统 模拟线程切换  
8.2 操作系统 进程线程结构  
8.3 操作系统 进程线程链表  
8.4 操作系统 TEB PEB  
8.5 操作系统      kpcr 结构  
8.6 操作系统      TrapFrame 结构体  
8.7 操作系统      SSDT 表  
8.8 操作系统      驱动详解  
8.9 操作系统      swapcontext函数  
8.10 操作系统      SwapContext函数  
8.11操作系统       ntReadVirtualMemory  
8.12操作系统       kiSwapThread  
8.13操作系统       kiWaitListHead  
8.14操作系统       对象句柄及线程等待快  
8.15操作系统       线程等待机制  
8.16操作系统       等待块及SetEvent 函数  
8.17操作系统       keWaitSingleObject函数  
8.18操作系统       APC机制  
8.19操作系统       kiDeliveApc  
8.20操作系统       Apc函数的调度时机  
8.21操作系统       异常处理  
8.22操作系统       kiDispatchException函数  
8.23操作系统       3环异常处理过程  
8.24操作系统       回调机制  
8.25操作系统       句柄  
8.26操作系统       对象句柄  
8.27-3.41项目（内核重载）  
8.42操作系统      调试机制  
8.43操作系统       Debug\_Object 结构  
8.44操作系统       创建调试对象函数  
8.45操作系统       发送调试消息函数  
8.46操作系统       DbgKpSendApiMessage 函数  
8.47操作系统       调试寄存器  
8.48操作系统       挂钩DbgKpSendApiMessage   
8.49操作系统       文档视图  
8.50操作系统       消息机制  
8.51操作系统       消息机制  
8.52操作系统       消息机制  
项目（3环调试器）  
  
第九章  毕业课题与综合实战   5000元  
1.xuetr 内核工具开发  
2.驱动级的任务管理器  
3.逆向调试各类exe软件成汇编代码或伪C源码  
4.病毒分析、木马分析、软件后门检测、病毒修复工具开发  
5.软件破解与加密  
6.游戏外挂/辅助的技术分析、多开/防多开、游戏驱动检测、游戏安全  
7.某社交软件HOOK技术分析  
8.给成品软件增加菜单/功能等插件