课程主要内容

一、试题类型

1、单选题

2、判断题

3、填空题

4、简答题

5、综合分析题

二、基础知识

1、病毒的定义、分类、生命周期、特性；

2、病毒对抗技术的方式以及各自的特定；

三、PE病毒

1、PE病毒的定义，常见的PE文件类型；

2、PE文件的判别；

3、PE文件格式解析（标识的值及所在位置，dos头、dos hub、PE文件头、PE可选头、节表、数据目录等重要字段的值及其含义）；

4、导入（引入）表、导出（引出）表的定位以及解析；

5、RVA到FOA的转换过程；

6、往PE文件中插入病毒代码的3种主要方式，掌握每种方式的过程以及对重要字段的修改；

7、病毒代码运行过程中需要解决的问题（需要自身动态获取要加载的模块以及模块中函数的地址，问题转换为要去动态寻找loadlibrary函数所在模块的基址，掌握获取该基址的4种方式的原理）；

8、重定位的原理以及代码实现；

9、动态获取API函数地址的原理以及代码实现；

9、熟练掌握实验中（PPT中），GetProcAddress函数的汇编代码实现过程；

四、引导型病毒

1、引导型病毒的定义；

2、CHS方式访存的原理以及缺陷；

3、莫里斯病毒、振荡波病毒、CIH病毒、大麻病毒的主要特点；

4、主引导扇区的结构、MBR代码的主要功能；

5、DPT表的数据解析（每个分区表项16字节的含义）；

6、引导型病毒的工作环境、工作原理；

7、系统的正常启动过程以及感染了引导型病毒之后的启动过程；

8、熟练掌握int 13 中断的功能以及运用；

9、实模式下1M内存的组成

10、常驻内存高端的原理、hook int 13 中断的原理

五、蠕虫病毒

1、蠕虫病毒的概述，32位cdecl调用约定的特点，shellcode的定义以及特点；

2、结合PPT上的“打开记事本”例子：熟练掌握缓冲区溢出的原理，会画函数栈帧的图

3、payload（填充区域、覆盖返回地址、shellcode）的组成以及各部分主要关注的问题，PPT上加强shellcode通用性的代码原理；

六、木马

1、文件型病毒与蠕虫病毒的区别；

2、木马的组成、入侵过程、自启动的方式、建立隐蔽通道的方式；

3、木马通常具备的功能，木马查找的主要工具；

总体题目不难，但要认真复习才能过，代码会考实验中的。