第三章 恶意代码及其分类

1）恶意代码与正常软件安全问题的差异；

2）恶意代码攻击目的；

3）恶意代码攻击目标；（**定点攻击、群体攻击**）

4）恶意代码功能；（**获取数据：静态、动态**）

5）计算机病毒与蠕虫定义（**典型例子、各自特点、两者差异**）

6）木马与后门定义（**典型例子、各自特点**）

7）刑法285、286修正案（七）的司法解释（**情节严重的情形**）

第四章 PE文件格式（仅了解）

1）PE文件格式总体结构

2）Optional Header关键信息

3）Image-Base、RVA、文件中节对齐、内存中节对齐；

4）Address-Of-Entry-Point的作用

5）通过函数名定位函数导出地址

第五章 Windows PE病毒

1）什么是感染、感染目标类型、感染思路

2）关键技术（**重定位、API函数获取、目标检索、感染**）

3）**重定位方法（简单汇编语言理解）**

4）kernel32模块基地址获取方法（**利用程序返回地址检索、利用PEB数据获取**）

6）搜索目标进行感染简单算法

7）文件感染具体方式

8）**增加新节感染的步骤**

9）**捆绑式感染（优缺点）**

11）**PE病毒感染实验：**

汇编链接命令中，代码节可写入的方法；

代码重定位的两种不同写法；

理解kernel32.dll基地址定位代码的代码；

获取kernel32.dll基地址后，根据函数名获取函数地址的流程；

第六章 宏病毒与脚本病毒

1）宏病毒概念

2）**宏病毒如何获得控制权**

3）宏病毒代码的主要部分（**简单宏理解、自我保护、感染-代码导出、代码导入**）

4）**脚本病毒感染文件的方法（简单脚本理解）**

5）脚本病毒对抗反病毒软件的几种技巧（**自加密、execute、修改对象声明、关闭反病毒**）

第七章 木马与后门（仅了解）

1）木马的基本概念、特点

2）木马的分类（信息获取型、破坏型）

3）木马植入方式（网页、邮件、文档、伪装、捆绑、其他）

4）木马通信方式及优缺点

5）远程控制木马常见功能与意图

6）木马检测思路

第八章 蠕虫（仅了解）

1）莫里斯蠕虫（利用的漏洞、惩罚）

2）蠕虫四个主要功能（信息搜集、扫描探测、攻击渗透、自我推进）

第九章 恶意代码的检测技术

1）检测对象、检测策略

2）**特征值检测**（掌握BM算法、AC算法、Veldman算法、Wu-Manber算法的使用）

3）**校验和检测**（思路、实用方法、检测对象、优缺点）

4）静态启发扫描（可疑指令、**系统调用DLL名称及对应功能**、启发式扫描步骤、优缺点）

隐藏策略（代码变形）

5）动态检测技术（虚拟机检测）

6）主动防御技术（常见可疑行为、优缺点）