7 恶意代码概述

7.1 恶意代码的定义

7.2 恶意代码的功能 (了解)

7.3 恶意代码的分类以及关键特点 (重点)

常见的恶意代码的类别

文件感染型病毒和漏洞利用型蠕虫的区别

木马和后门的概念

7.4 恶意代码与网络犯罪（重点）

根据法律条文认定某人利用恶意代码进行危害的行为

8 PE 文件结构 （重点）

8.1 PE 文件及其表现形式

常见的 PE 文件有哪些?

8.2 PE 文件格式与恶意软件的关系

PE 病毒的特点/功能：感染，控制权获取、不破坏原有文件的功能和形态

8.3 PE 文件格式总体结构

掌握关键数据结构的含义和作用比如 image base

掌握文件和内存中对齐的大小

节表的作用

8.4 代码节与数据节

代码节和数据节的一般属性作用

8.5 引入函数节：PE 文件的引入函数机制

掌握定位引入目录表起始位置的方法

如何根据引入目录表找到指定函数地址的步骤?

8.6 引出函数节：DLL 文件的函数引出机制

掌握定位导出函数节的方法

已知函数名如何在定位导出函数地址的 RVA/PFile 以及序号?

8.7 资源节：文件资源索引、定位与修改

作用是什么？

8.8 重定位节：镜像地址改变后的地址自动修正

作用是什么？

9 PE 文件病毒（重点）

9.1 PE 病毒的基本概念

感染的定义

9.2 PE 病毒的分类

感染的目标类型

9.3 传统文件感染型

关键技术：重定位

关键技术：kernel dll 基址获取方法（掌握方法 1 和方法 3，了解方法 2 和方法 4）

目标搜索

感染和控制权获取的方法

9.4 捆绑释放型

优缺点和基本原理

9.5 系统感染型病毒

了解传播方式和获取控制权的方式

10 宏病毒和脚本病毒

10.1 宏的基本概念与使用

10.2 宏病毒的传播方法

掌握宏病毒传播原理

10.3 宏病毒的自我保护

了解宏病毒常见**自我保护**的方法

10.4 VBS 脚本的概念及使用

了解 VBS 脚本的功能

脚本病毒和 PE 病毒的区别

10.5 VBS 脚本病毒的感染技术

了解感染和传播方式

10.6 VBS 脚本病毒的变形技术

了解常见的变形方法

11 木马

11.1 木马的基本概念

木马和后门的异同

11.2 木马的分类

了解木马的不同分类方式 行为视角、功能视角

11.3 木马的植入方式

了解常见的植入方式

11.4 木马的通信方式

掌握木马的通信方式和优缺点

11.5 木马的主要功能及意图

了解远控木马的常见功能

11.6 木马检测思路

了解从木马检测的常见特征

12 网络蠕虫

12.1 网络蠕虫的定义

蠕虫和病毒的区别

12.2 网络蠕虫的分类

了解常见蠕虫的分类

12.3 网络蠕虫的功能结构与关键技术（漏洞利用型）

了解蠕虫的基本的功能和特点

12.4 网络蠕虫的检测与防治

常见的防范措施

13 恶意代码防治与检测技术

13.1 恶意代码检测对象与策略

了解常见的检测对象和检测技术

了解几种方法的优缺点和基本原理

13.2 特征值检测技术

13.3 校验和检测技术

13.4 启发式扫描技术

13.5 虚拟机检测技术

13.6 主动防御技术