《软件安全》

课程教学大纲

一、 课程基本信息

课程类型	专业必修课	☑理论课（含上机、实验学时）			
		□实习 □课程设计 □毕业设计			
课程编码	7232701	总学时	32	学分	2
课程名称	软件安全				
课程英文名称	Software Security				
适用专业	信息安全				
先修课程	（7240911）信息安全、（7044811）汇编语言程序设计、 （7001631）C 程序设计				
开课部门	信息学院计算机系				

二、 课程性质与目标

本课程为信息安全专业必修课，其概念、理论及分析技术广泛应用于计算机病毒对抗等诸多领域。通过本课程的学习，不仅使学生掌握计算机病毒的编写理论与技术，而且通过对计算机病毒编写理论的学习，更好的提升学生在计算机病毒对抗领域中实施病毒检测、分析和处置能力，为我国网络安全培养合格的软件安全对抗人才。

课程目标 1：学生应掌握计算机病毒的编写理论与关键技术；

课程目标 2：学生应能提升自身在计算机病毒对抗领域中实施病毒检测、分析和处置能力；

课程思政目标：充分发挥课程所承载的育人功能，加强选课学生保卫我国网络空间的主权意识，培养合格的软件安全对抗人才。同时，提升学生的法律意识、加强品德修养，坚定学生理想信念、厚植爱国主义情怀，教育其所学技术仅能用于合法范畴，为国创新。

三、 课程教学基本内容与要求

1. 绪论

本章主要讲授计算机病毒的定义、特征、分类以及历史发展，让学生对计算机病毒有一个初步的印象，明确学习本课程的意义——“更好的分析、处置计算机病毒”。本章要求学生对知识点的具体掌握程度如下：

（一）掌握：计算机病毒的定义、特征、分类

（二）理解：计算机病毒的本质

（三）了解：计算机软件安全性问题的来源、产生、演化与发展

2. 预备知识

本章主要讲授计算机病毒相关的预备知识，主要包含：磁盘系统、文件系统、PE 文件格式以及计算机引导过程。通过这些预备知识，为后续学习相关的计算机病毒编写技术打好基础。本章要求学生对知识点的具体掌握程度如下：

（一）掌握：FAT32 文件系统、NTFS 文件系统，PE 文件格式

（二）理解：磁盘结构、引导扇区

（三）了解：计算机引导过程

3. 计算机病毒的基本机制

本章主要讲授计算机病毒的组织结构、计算机病毒生命状态转换、计算机病毒的三种机制：传播机制、触发机制、破坏机制。本章要求学生对知识点的具体掌握程度如下：

（一）掌握：计算机病毒的传播机制、触发机制与破坏机制

（二）理解：计算机病毒的基本组成结构

（三）了解：计算机病毒的传播途径

4. DOS 病毒分析

本章主要讲授引导型病毒，分析其构成结构及每个表项字节的含义，此外讲解 DOS 环境下的文件病毒和混合病毒。本章要求学生对知识点的具体掌握程度如下：

（一）掌握：引导型病毒原理

（二）理解：MZ 文件格式

（三）了解：DOS 系统中文件型病毒

5. Windows 病毒分析

本章主要讲授 windows PE 病毒、宏病毒、脚本病毒、网页病毒定义、特征及所使用的技术，特别是 windows PE 病毒的感染技术，涉及重定位技术、API 地址获取技术，以及宏病毒、脚本病毒的自我隐藏技术等。本章要求学生对知识点的具体掌握程度如下：

（一）掌握：重定位技术、函数内存空间定位技术

（二）理解：Windows PE 病毒、宏病毒、脚本病毒

（三）了解：Windows 病毒的分类

6. 病毒技巧

本章主要讲授计算机病毒的隐藏技术、花指令技术、变形病毒技术与多态病

毒技术、加壳等自我保护技术等。本章要求学生对知识点的具体掌握程度如下：

（一）掌握：计算机病毒的自我保护技术

（二）理解：多态和变形的区别

（三）了解：花指令

7. 漏洞与网络蠕虫

本章主要讲授漏洞产生的原因与漏洞挖掘技术、网络蠕虫病毒的特征、一些内存溢出技术等。本章要求学生对知识点的具体掌握程度如下：

（一）掌握：网络蠕虫概念与技术、内存溢出概念及成因

（二）理解：堆喷射技术

（三）了解：一些经典的网络蠕虫

8. 特洛伊木马与 Rootkit

本章主要讲授木马原理与木马的编写技术，重点讲解远程线程注入技术等。本章要求学生对知识点的具体掌握程度如下：

（一）掌握：木马的远程线程注入技术

（二）理解：木马的运作方式、自启动方式

（三）了解：木马概念及技术的发展趋势

四、 课程学时分配

教学内容	讲授	实验	课内学时小计
1.绪论	2		2
2.预备知识	6	2	8
3.计算机病毒的基本机制	2		2
4. DOS 病毒分析	2		2
5. Windows 病毒分析	4	2	6
6.病毒技巧	4	2	6
7.漏洞与网络蠕虫	2		2
8.特洛伊木马与 Rootkit	2	2	4
合　　计	24	8	32

五、 实践性教学内容的安排与要求

本课程主要包括 PE 文件剖析实验、Windows 恶意代码剖析实验、变形/多态

恶意代码实验和键盘监听木马实验，通过实验，学生应全面掌握软件安全的理论与基本技术，将理论和实际应用切实结合起来。**其中:**“变形/多态恶意代码实验”学生从变形恶意代码和多态恶意代码两类任选其一进行实验即可。

1. PE 文件剖析实验（验证性实验） 2 学时
2. Windows 恶意代码剖析实验（验证性实验） 2 学时
3. 变形/多态恶意代码实验（验证性实验） 2 学时
4. 键盘监听木马实验（验证性实验） 2 学时

六、 教学设计与教学组织

本课程所涉计算机病毒相关知识较多，具有知识点多、涉及面宽、内容跨度大、综合思考能力要求高等特点。因此在抓好课堂教学效果的同时，应做好课前预习和课后复习及实验验证环节，需要认真完成书面作业及思考题，并通过增强师生间、同学间的多种形式的讨论（如课后答疑、课下讨论、网上讨论等）来提高课程的教学效果和教学质量。

课程教学方法及具体要求如下：

1. 课堂讲授

1）以能力培养为导向，注重理解各类计算机病毒的实现原理。为保证教学质量，课堂讲授中应重点突出、点面结合，既要保证完成使广大学生接受完整的计算机病毒知识的教学目标，又要针对关键重点内容作较为详尽的透彻讲解，使学生真正领会和掌握本课程的知识要领及技术要点。

2）注重实践环节。为使学生能够深入理解计算机病毒原理，设计良好的验证性实验，加深学生对基础知识的理解。

3）多媒体课件与板书结合的教学手段与多种教学方法兼施并用。教学方法则采取在教师讲授基本教学内容的过程中适当穿插引入个体针对性提问、集体提问、答疑、讨论等教学形式。

2. 讨论

鼓励同学之间或同学与教师之间针对计算机病毒的重点和难点内容展开讨论，以澄清知识要点、扩大知识面和培养独立思考能力及创新能力。

3. 课前预习和课后复习

每次课前预习时间应不少于相应教学内容的课堂讲授计划时间，课后复习以课堂讲授内容为主线、完成相应作业为突破口。同时，鼓励学生自主参加 CTF 比赛或 pwn 类型题目的学习，从而更好地掌握该课程的内容。

七、 教材与参考资料

1.教材

《计算机病毒分析与对抗》（第 2 版），傅建明、彭国军、张焕国著，武汉大学出版社，2009 年 12 月，ISBN：9787307074002

2.参考资料

（1）《计算机病毒揭秘与对抗》（第 1 版），王倍昌著，电子工业出版社，2011 年 10 月，ISBN：9787121146053

（2）《计算机病毒与恶意代码——原理、技术及防范》（第 4 版），刘功申、孟魁、王轶骏、姜开达、李生红著，清华大学出版社，2019 年 05 月，ISBN：9787302516583

（3）《论网络空间主权》（第 1 版），方滨兴著，科学出版社，2020 年 04 月，ISBN：9787030542557

八、 课程考核方式与成绩评定标准

采用百分制，总评成绩由平时成绩、实践教学成绩和期末成绩三部分组成，平时成绩占 20% ，实践成绩占 20%，期末考试成绩占 60%。

九、 大纲制(修)订说明

无

大纲执笔人：杜春来

大纲审核人：李琛

开课系主任：肖珂

开课学院教学副院长：宋威

制（修）订日期：2022 年 2 月