《软件安全实验》课程大纲

一、课程名称（中英文）

中文名称：软件安全实验

英文名称：Software Security Experiment

二、课程代码

SCS0004

三、学时与学分

总学时：16 学时

总学分：1 学分

四、先修课程与后续课程

先修课程：《数据结构》、《C 语言程序设计》、《汇编语言》

后续课程：《计算机网络安全》、《无线网络安全》、《WEB 安全技术》、《工业网络安全综合实践》、《网络安全程序设计》、《计算机网络与安全工程实践》

五、教材与教辅

自编实验指导书

六、适用学科专业

信息安全

七、课程简介

《软件安全实验》是配合《软件安全》课程独立开设的实验课，面向（网络空间安全）信息安全专业和网络空间安全专业学生开设。目的在于通过一系列实验，帮助学生理解和掌握软件安全中的基础理论知识和核心技术，掌握恶意代码的概念，复制、传播、感染、隐藏等基本原理，并进一步培养学生对软件漏洞挖掘与利用的实际能力，掌握恶意代码查杀流程以及查杀的基本算法。系列实验包括基础实验、验证性实验、综合性实验和创新性实验。

八、课程目标

课程的具体目标包括：

目标 1：在理解恶意代码概念的基础上，根据任务要求，设计方案，完成代码，并分析复制、感染、传播的原理，比较不同传播技术的差别。同时，依据设计方案，开发满足用户特定安全需求的信息系统或信息安全部件，并对其进行详细分析、比较与优化，以确保系统具备较强的安全性、可靠性和高效性，能够有效应对潜在的恶意代码威胁。

目标 2：在了解软件安全最新态势以及国内外前沿软件安全利用和防御技术的发展基础上，结合相关的管理手段，分析这些技术在实际应用中对软件效率的负面影响、以及由此带来的额外开销和局限性，全面评估其在实际环境中的适用性和有效性。同时，能够理解通过技术与管理手段降低这些负面影响的作用与局限性，权衡安全性与效率之间的平衡，以便为系统设计和安全策略的优化提供有效的指导。

九、教学内容与教学环节

实践实验 1:综合利用之逆向工程

本章节将综合利用之前的 Pwntools 工具实践与 ELF 文件格式，详细分析如何对指定 ELF 文件进行逆向分析，并寻找其中存在的敏感信息。通过实际的案例分析，熟练掌握逆向工程的工作原理与技巧、代码调试技巧等内容。

1. 教学内容

1）编写代码独立解析 ELF 文件，获取 ELF 文件元信息；

2）使用进程分析工具独立分析给定 ELF 的进程地址空间；

3）通过对 ELF 程序进行逆向分析，获取程序中的敏感信息（如 flag）。

2. 教学目标

1）利用实例掌握 ELF 二进制文件的逆向工程与进程调试方法。

3. 教学重点

1）熟练掌握 ELF 文件格式解析与进程调试；

2）逆向工程中的关键技术和工具的使用。

4. 教学环节

围绕教学重点和教学难点，综合应用课堂讨论、作业、课外实践、课外阅读等教学形式。

1）课堂讨论

围绕 ELF 文件结构与逆向工程展开，讨论如何利用逆向分析工具获取程序的敏感信息。

2）作业

学生需编写代码独立解析 ELF 文件，获取 ELF 文件的元信息，并使用 GDB 等工具进行进程地址空间分析。

3）课外实践

以小组为单位对给定 ELF 可执行文件（如 easy_re）进行逆向分析，获取程序中的 License，并在实践平台进行验证。

4）课外阅读

推荐阅读与逆向工程、ELF 文件结构、GDB 调试等相关书籍和文档，深入理解逆向工程的基本原理和实践应用。

实践实验 2 综合利用之防御绕过

本章节将详细分析漏洞利用的防御机制（如栈保护，ASLR 等）的缺点与绕过技巧，并通过实际案例分析，帮助实践并熟练掌握这些防御机制的绕过方法。

1. 教学内容

1）学习并掌握栈保护、数据执行保护（DEP）、地址空间布局随机化（ASLR）、Fortify Source 等常见防御机制；

2）了解这些防御机制的缺陷，以及攻击者如何利用这些缺陷进行绕过，如 ROP 技术绕过 DEP、byte-by-byte 爆破绕过栈保护等；

3）使用 Pwntools、ROPgadget 等工具编写 ROP 链，获取具有任意命令执行功能的 Shell；

4）结合案例分析，深入理解如何绕过这些防御机制并实践其绕过过程。

2. 教学目标

1）通过实践案例掌握常见防御机制的缺陷及其绕过技巧；

2）学习如何利用高级漏洞利用技术绕过现代操作系统的防御措施，理解攻防对抗中的防御机制的局限性。

3. 教学重点

1）栈保护、DEP、ASLR、Fortify Source 等防御机制的原理与实现；

2）通过编写 ROP 链及利用 byte-by-byte 爆破等技术绕过防御机制的实践过程。

4. 教学难点

1）防御机制的缺陷及绕过手段的精确实现；

2）在不同操作系统及环境下，如何有效利用 ROP 链及其他高级技术绕过防御措施。

5. 教学环节

围绕教学重点和教学难点，综合应用课堂讨论、作业、课外实践、课外阅读等教学形式。

1）课堂讨论

围绕栈保护、ASLR、DEP 等防御机制展开，讨论这些防御机制的优缺点及其在实战中的有效性。

2）作业

学生需独立或以小组为单位完成漏洞实例分析，定位软件漏洞所在位置与成因，利用 byte-by-byte 爆破机制对栈保护防御进行绕过，并编写 ROP 链获取具有任意命令执行功能的 Shell。

3）课外实践

要求学生使用 Pwntools 库编写漏洞利用脚本，对已知的简单漏洞进行攻击，演练绕过栈保护或 DEP 等防御机制。链构造等方式实现防御机制的绕过，并在实践平台进行验证。

4）课外阅读

推荐阅读与漏洞利用防御绕过相关的书籍和文档，深入理解现代操作系统中的防御机制及其对抗策略，包括 "Buffer OverFlow Attacks: Detect, Exploit, Prevent" 和 "Return-oriented programming without returns"。

实践实验 3：病毒的自我复制实验

1.教学内容

1）设计并开发可自我复制的病毒来理解病毒自我复制的原理

2）利用亲手编写的病毒来观察并掌握病毒复制的全部文件操作流程

3）在不限制复制次数的情况下观察它的破坏效果

2.教学目标

1）帮助学生深入理解计算机病毒的自我复制机制，并掌握防范病毒攻击的基本原理和技术；

2）课程思政：让学生避免触及法律的红线，并树立正确的网络安全意识。

本实践实验支持的课程目标为目标 1、目标 2。

3.教学重点

理解病毒的自我复制原理，并掌握病毒复制的文件操作流程

4.教学难点

传播病毒的文件共享权限获取问题

5.教学环节

1）作业

学生独立开发自己编写的病毒程序，并演示病毒的自我复制过程。

2）课外阅读

阅读《计算机病毒与恶意代码》刘功申。

实践实验 4：恶意代码查杀实验

1.教学内容

1）理解恶意代码查杀流程

2）掌握查杀基本算法

3）基本掌握特征码、校验和、简单启发查杀技术

2.教学目标

1）帮助学生深入理解恶意代码的行为特征及其查杀方法，并掌握查杀工具的使用和手动分析恶意代码的技巧；

2）课程思政：引导学生遵守法律法规，树立正确的网络安全意识，避免触犯法律底线。

本实践实验支持的课程目标为目标 1、目标 2。

3.教学重点

掌握恶意代码查杀流程以及查杀基本算法

4.教学难点

病毒查杀需要一定的时间形成自己的经验，且特征码精简与准确性难以保证

5.教学环节

1）作业

演示恶意代码查杀的命令行程序 MiniAntiVirus，并对某文件夹中的文件进行病毒查杀；最后通过分析工具，找出同组人编写的病毒模拟程序的特征串，通过特征串扫描，对该模拟程序进行识别，并报

出该病毒名称、染毒文件名、文件创建时间、文件大小、文件位置等信息。

2）课外阅读

阅读《计算机病毒与恶意代码》刘功申。

十、学时分配

序号	主要内容	课内学时	课外学时
实验一	综合利用之逆向工程	4	
实验二	综合利用之防御绕过	4	
实验三	病毒的自我复制实验	4	
实验四	恶意代码查杀实验	4	
总计		16	

十一、教学策略

主要的教学环节包括讲解实验要求和重难点，学生实验，过程辅导，验收问答，实验报告批阅等阶段。

1.教学方法

本课程的教学方法主要体现在如下几个方面：

1）以课程讲解为辅助，以实题和实践为主要手段，通过现实中的漏洞实例进行实战训练，让学生直接体验逆向、分析、漏洞挖掘和利用技术；

2）引导学生自主创新，面对实战漏洞，通过对实战漏洞的分析讨论，各小组汇报解决方案，教师对方案进行点评等一系列过程，让学生在了解一般性方法的同时，提出一些有新意的思路，对创新型思路给予加分；

3）因材施教，难易适中，各实践、实验均安排选做加分内容，鼓励特色创新，激发学习热情,提升学生自主学习能力；

4）制定完善、公正的实验结果评判标准，通过建立课程检查表，量化实践、实验系统性能指标，提

升实践、实验结果评价的科学性、合理性；

5）引导学生逐步形成软件安全的分析能力。软件安全的分析能力是安全综合能力的主要部分，从全面到局部的顺序来审视安全问题，为走向安全工作岗位以及安全研究人员培养安全的分析思维。

2.学习方法

“软件安全实验”是一门理论性、技术性和实践性高度融合的专业核心课程。学习过程中，首先要注重对安全基础知识和常见漏洞的深入理解，重点研究各类漏洞的成因、危害及防御措施，全面掌握软件安全的基本理论和核心技术。其次，结合先修课程如 C 语言程序设计、数据结构、汇编语言等内容，将前期知识灵活运用于软件安全问题的分析和解决中。第三，积极参与课程安排的实验项目，独立完成漏洞分析、漏洞修复和安全工具的使用，通过实验训练实践动手能力，增强发现问题、分析问题和解决问题的能力，培养对软件安全问题的敏感性和应对策略。

十二、课程评价

1.课程成绩构成

课程成绩由传统的终结性评价向过程评价转变，形成性评价中平时成绩所占比例要加大；

实验检查成绩：50%。包括按时参与实验、实验设计思路、实现结果的展示、实验结果的分析等内容。

实验报告：50%。为总结报告的形式，具体评分标准见表 2。

表 1 软件安全实验课程考核与成绩评定

课程目标	考核与评价方式及成绩占所在项的比例(约)	
	实验检查成绩	实验报告
1	50%	50%
2	50%	50%
总成绩	实验检查成绩×0.5+终结性考试成绩×0.5	

表 2 实验报告评分标准

项目	实验报告评价方式及成绩占所在项的比例(约)		
	撰写规范	实验过程	问题分析与小结
1	20%	50%	30%
总成绩	撰写规范×0.2+实验过程×0.5+问题分析与小结×0.3		

2.考核与评价标准（实验报告评分标准见表 2）

（1）课程目标 1 的评价标准

实验检查成绩**评价标准**			
优秀	良好	及格	不及格
依据设计方案，开发满足用户特定安全需求的信息系统或信息安全部件，并进行分析、比较和优化。	能够依据设计方案，较好开发出符合用户特定安全需求的信息系统或信息安全部件。并对系统的各个方面进行较为系统的分析，能够精确比较不同设计的优缺点，有效地提出优化方案。	能够根据设计方案开发出基本符合用户特定安全需求的信息系统或安全部件。虽然系统功能基本完整，但在某些方面的安全性或性能优化存在不足。能够进行一定程度的分析和比较，但优化策略较为有限，改进空间较大。	不能根据设计方案开发出符合用户特定安全需求的信息系统或安全部件。系统开发过程中存在严重问题，功能不全或安全性不足，无法满足用户需求。缺乏有效的分析和比较，对系统的优化欠缺理解或不能提出可行的改进措施。

（2）课程目标 2 的评价标准

实验检查成绩**评价标准**			
优秀	良好	及格	不及格

能够理解用技术、管理手段降低负面影响的作用与其局限性。	能够较好理解技术和管理手段在减少信息安全领域负面影响中的重要作用，准确识别其应用场景与局限性。	对技术和管理手段在降低负面影响中的作用有基本的理解，能够识别常见的局限性，但分析不够深入。	不能有效理解技术和管理手段在降低负面影响中的作用，无法识别其局限性。选择和应用技术或管理措施时缺乏针对性，难以形成可行的解决方案。