

目 录

1. 涉密信息系统管理.....	1
2. 软件安全基础.....	3
3. 保密技术.....	5
4. 网络安全实验.....	7
5. 面向对象程序设计.....	9
6. 计算机病毒防护技术.....	11
7. 网络攻防实验.....	13

涉密信息管理系统实验教学大纲

一、实验基本信息

课程编号：201421103

中文名称：涉密信息管理系统

英文名称：Management of Secrecy Information System

课程性质：专业核心课程

面向专业：信息安全

开设学期：3

课程总学时：32

实验学时：8

是否独立设课：否

二、实验目的和任务

本课程主要以涉密信息系统工程建设的核心内容，涉及信息管理系统理论、涉密信息系统防护与检查、危害入侵与侦测等，通过本课程的学习，使学生掌握信息管理系统的基础知识、了解信息安全保密技术，培养良好的保密业务素质。通过实验过程的学习，让学生掌握涉密信息工程建设的基本流程，了解涉密信息系统运行使用的制度及规定，规范涉密信息系统应用行为。

三、实验教学基本要求

了解保密技术国产化与国际信息安全环境的关系，深入研讨棱镜门，维基解密案件的本质。

了解涉密信息系统种类，以及计算机常见的安全检查方法，熟悉安全保密检查的操作流程。

四、实验项目基本情况

序号	实验项目名称	实验学时	内容提要	实验类型	实验要求
1	失窃密工具应用	4	实际动手操作失窃密工具，撰写体验报告	演示型	必做
2	计算机安全保密检查与操作	4	掌握计算机安全保密检查与操作	综合型	必做

五、实验教材（指导书）或网络资源

[1] 孙建国 编著. 涉密信息安全保密管理. 金城出版社, 2014

[2] 孙建国 韩启龙 编著. 网络安全实验教程（第二版）. 清华大学出版社, 2014

六、考核方式

小论文。

软件安全基础实验教学大纲

一、实验基本信息

课程编号：201421106

中文名称：软件安全基础

英文名称：Foundation for software security

课程性质：专业核心课程

面向专业：信息安全

开设学期：6

课程总学时：32

实验学时：6

是否独立设课：否

二、实验目的和任务

《软件安全基础》课程是信息安全专业的必修课程，实验是一项重要的实践教学内容，是本课程的综合技能训练课。通过实验，加深理解、验证、巩固课堂教学内容，提高学生在开发应用程序、web 编程、网络编程与数据库编程时能够保障程序安全运行的实际应用能力，加深学生对缓冲区溢出、内存溢出、跨站脚本攻击等技术方面概念的理解，掌握安全编程的方法和基本措施。通过实验，培养学生在安全编码方面的能力、软件测试方面的能力，并提高了学生独立解决问题的能力。

三、实验教学基本要求

1. 学会发现常见的函数中可能发生的缓冲区溢出漏洞，学会用常见的反汇编软件发现缓冲区溢出问题，并能够利用此缓冲区溢出，改变程序流程，达到攻击目的。
2. 通过模拟一个邮件点击链接的攻击过程，攻击者给客户发送一个邮件，客户点击邮件，攻击者窃取客户的信息，使学生学会在实际 web 编程中应该避免出现的 web 安全漏洞。
3. 搭建数据库，设计好数据库表，设计攻击代码——也就是将恶意代码插入常用的数据库语句中，然后将该字符串传递给数据库服务器执行，根据数据库返回结果，窃取或者篡改数据库用户信息。

四、实验项目基本情况

序号	实验项目名称	实验学时	内容提要	实验类型	实验要求
1	内存安全	2	1、学会使用反编译软件 OllyDBG; 2、分析缓冲区溢出发生的地方; 3、编写恶意代码, 在发生缓冲区溢出的地方执行。	基本型	必做
2	Web 编程安全	2	1、搭建 Tocat 服务器; 2、搭建 IIS 服务器; 3、编写 ASP 和 JSP 脚本; 4、模拟跨站脚本攻击过程。	基本型	必做
	SQL 注入攻击	2	1、搭建 MySQL 数据库; 2、设计数据库; 3、用 JDBC 连接数据库; 4、编写 ASP 脚本攻击数据库。	基本型	必做

五、实验教材（指导书）或网络资源

[1] 郭克华 1, 王伟平 2, 刘伟 3. 软件安全实现: 安全编程技术 (第一版). 清华大学出版社, 2010

[2] 王清 1, 张东辉 2, 周浩 3. Oday 安全: 软件漏洞分析技术 (第二版). 电子工业出版社, 2011

六、考核方式

课堂实验检查评分

保密技术实验教学大纲

一、实验基本信息

课程编号：201421109

中文名称：保密技术

英文名称：Secrecy Technologies

课程性质：专业核心课程

面向专业：信息安全

开设学期：6

课程总学时：32

实验学时：20

是否独立设课：否

二、实验目的和任务

本实验课的目的是让学生将理论知识应用到实践中来，从而起到加深、巩固理论知识，提高学生的设计能力和学习兴趣。通过课程实践，使学生能熟悉课程中应用的技术及实验设施，亲自动手实现保密技术相关的验证和设计工作，为学生完成后续专业实验课奠定基础。

三、实验教学基本要求

本实验是在学生完成保密技术理论课程的基础上进行，以巩固和应用相关理论知识点，培养学生具备利用理论知识解决实际问题的能力；通过实验使学生能够按要求对各个知识点实验进行独立验证和设计，并归纳解决实验过程中的问题和解决思路，形成实验报告。

四、实验项目基本情况

序号	实验项目名称	实验学时	内容提要	实验类型	实验要求
1	操作系统保密防护配置实验	4	系统安全策略、安全模版的配置；用户管理和用户组策略管理；系统审核与安全扫描；服务安全配置	基本型	必做
2	服务器安全配置实验	4	Web、FTP 服务器在 windows 或者 linux 平台下的安全配置	基本型	必做
3	用户访问控制实验	4	设计一个用户访问控制方案，完成自主访问控制、身份认证、基于等级的访问控制和基于角色的访问控制功能	综合设计型	必做

序号	实验项目名称	实验学时	内容提要	实验类型	实验要求
4	保密检查实验	4	设计一个针对 windows 平台的保密检查方案，评估系统的保密防护措施和可能泄密途径	综合设计型	必做
5	内容安全审计实验	4	设计一个内容安全审计方案，对特定类型的文件内容进行审计，评估内容泄密的可能性。	综合设计型	必做

五、实验教材（指导书）或网络资源

- [1] 冯光升. 保密技术自编讲义.
- [2] 冯光升等. 信息系统安全实验. 哈尔滨市：哈尔滨工程大学出版社，2014.
- [3] 赵战生、杜虹、吕述望. 信息安全保密教程. 合肥市：中国科学技术大学出版社，2006.
- [4] 黄月江、祝世雄. 信息安全与保密(第2版). 北京：国防工业出版社. 2008.

六、考核方式

教学基本要求项	考核形式	占总成绩的比例
考查学生对保密防护技术、保密检查技术的掌握程度，以及是否具备采用工具进行泄密检查和保密防护	实验报告	60%
考查学生是否具备系统性的保密技术知识体系结构、是否初步在涉密网络集成、涉密信息系统中应用的能力	大作业	40%

网络安全实验实验教学大纲

一、实验基本信息

课程编号：201421201

中文名称：网络安全实验

英文名称：Networks Security Experiment

课程性质：专业实践环节

面向专业：信息安全

开设学期：6

课程总学时：32

实验学时：32

是否独立设课：是

二、实验目的和任务

通过实验使学生认识网络安全技术的基本概念、原理和技术，掌握基本的网络安全攻防技术，常用数据加密方法及入侵检测的原理和方法。加深对课堂教学的理解。培养学生的实验技能、动手能力和分析问题、解决问题的能力。

三、实验教学基本要求

通过本实验课程的学习，学生应达到下列基本要求：

- 1、了解计算机网络安全的重要性，建立网络安全意识。
- 2、掌握计算机网络安全方面的基本技术，能对系统的安全问题做出相应的对策。
- 3、掌握网络安全的防范技术。

四、实验项目基本情况

序号	实验项目名称	实验学时	内容提要	实验类型	实验要求
1	网络分析器应用实验	4	熟悉并熟练运用网络分析器，能够对网络数据进行分析	综合型	必做
2	远程控制实验	8	了解远程控制的基本原理，熟悉远程控制软件的使用	综合型	必做
3	入侵检测系统分析与应用	10	了解入侵检测系统，熟悉运用入侵检测软件，撰写入侵检测系统使用报告	综合型	必做
4	虚拟蜜罐分析与实践	10	掌握虚拟蜜网的定义、结构及具体搭建步骤。利用蜜网工具进行网络行为分析	综合型	必做

五、实验教材（指导书）或网络资源

[1] 孙建国, 韩启龙 编著. 网络安全实验教程 (第二版), 清华大学出版社, 2014

[2] <http://cetc.hrbeu.edu.cn>

六、考核方式

实验报告

面向对象程序设计实验教学大纲

一、实验基本信息

课程编号：201421302

中文名称：面向对象程序设计

英文名称：Object-Oriented Programming

课程性质：专业选修课程

面向专业：信息安全

开设学期：3

课程总学时：48

实验学时：16

是否独立设课：否

二、实验目的和任务

面向对象程序设计实验是验证、巩固和补充课堂讲授的理论知识的必要环节，加深学生对面向对象程序设计理论的理解，培养学生初步分析问题的能力，并在此基础上逐步掌握面向对象的编程方法和编程技巧，运用所学的理论知识解决实际问题的能力。

三、实验教学基本要求

要求学生掌握面向过程程序设计、模块程序设计、面向对象程序设计等概念，区分这些程序设计方法的不同点；理解面向对象程序设计的基本特性，例如数据抽象、封装、继承、多态性等；掌握面向对象程序设计语言 C++ 编程语言的基本结构；掌握类的概念，包括类、对象、成员函数等概念；掌握构造函数、析构函数的工作原理，以及定义和调用；理解程序运行时内存的分布情况，重点掌握动态对象的创建和撤销；掌握拷贝构造函数的运行机制；掌握静态成员和友元的概念，定义和调用；掌握运算符重载技术，简化某些类的使用；熟练掌握继承和多态的工作原理，以及设计思想，并采用该设计思想解决现实世界的实际问题；掌握模板的用法，包括类模板和函数模板的使用。

四、实验项目基本情况

序号	实验项目名称	实验学时	内容提要	实验类型	实验要求
1	C++语言基础	2	设计和实现带有过程化语句的程序；编写和实现入门程序；设计和实现矩阵的加法和倒置计算；设计和实现带	基本型	必做

			有指针、引用和函数的程序		
2	类和对象	2	设计和实现带有成员函数的程序；设置类内成员的属性和成员函数的访问边界，并设计程序访问不用访问边界的类内成员；设计构造函数初始化对象，析构函数清除对象	基本型	必做
3	动态对象的创建	2	设计并实现利用 <code>new</code> 和 <code>delete</code> 运算符动态创建和清除对象的程序	基本型	必做
4	拷贝构造函数	2	设计在函数中引入对象，采用拷贝构造函数传递对象的程序	基本型	必做
5	静态成员与友元	2	设计并实现带有 <code>static</code> 修饰的类内成员的程序，并编写代码访问这些类内成员；设计并实现带有友元的程序	基本型	必做
6	运算符重载	2	使用运算符重载技术编写程序，简化某些类的使用	基本型	必做
7	模板	2	使用模板技术编写一个多数据类型通用的类	基本型	必做
8	继承和多态	2	使用继承和组合技术进行代码重用；使用 <code>virtual</code> 进行多态的编程实践	综合设计型	必做

五、实验教材（指导书）或网络资源

《面向对象程序设计》教材[1]及主要参考资料[2-4]如下：

- [1] 游洪跃，伍良富等.C++面向对象程序设计教程. 清华大学出版社，2010年
- [2] 况立群，熊风光，杨晓文等编著. 面向对象程序设计. 清华大学出版社，2013年
- [3] 陶维安，顾和明，陈曦编著. 面向对象程序设计与实践. 西南交通大学出版社，2013年
- [4] 谭浩强编著.C++程序设计. 第2版. 清华大学出版社，2011年

六、考核方式

非独立设课，考核方式为演示实验结果计入平时成绩。

计算机病毒防护技术实验教学大纲

一、实验基本信息

课程编号：201421303

中文名称：计算机病毒防护技术

英文名称：Computer Virus Protection Technologies

课程性质：专业选修课程

面向专业：信息安全

开设学期：7

课程总学时：24

实验学时：4

是否独立设课：否

二、实验目的和任务

计算机病毒是引出信息安全问题的根本原因之一，计算机病毒防治是信息安全中非常重要的一个方面。所以计算机病毒的基本原理和计算机病毒防治的基本原理与方法都是信息安全专业的学生必须了解和掌握的基本内容。本教学环节的任务是以计算机及其操作系统为实验环境，结合计算机病毒的相关原理，以高级程序设计语言为基础，通过完成计算机病毒检测与清除技术实验和病毒程序与杀毒程序编程实验，掌握计算机病毒防治的基本方法与流程，使学生对计算机病毒的原理，方法，特性有更深刻的理解，进一步提高学生的动手能力、分析问题、解决问题的能力。

三、实验教学基本要求

通过该课程的教学，使学生熟悉计算机病毒的基本原理和计算机病毒防治的基本原理与方法，掌握计算机病毒检测与清除技术，运用所学知识设计和实现病毒程序与杀毒程序。具体要求如下：

1. 学习和掌握计算机病毒检测与清除技术。
2. 设计和实现一个病毒程序并编写相应的杀毒程序。
3. 能够通过本次设计培养学生一定的系统设计能力。
4. 每人提交一份 2000 字左右的实验报告书。

四、实验项目基本情况

序号	实验项目名称	实验学时	内容提要	实验类型	实验要求
1	计算机病毒检测与清除技术实验	2	掌握典型病毒的检测方法和清除方法： 1. 熊猫烧香病毒 2. 威金病毒	综合型	必做
2	病毒程序和杀毒程序编程实验	2	掌握病毒程序和杀毒程序编程方法，编程实现一个简单的病毒程序，并编写杀毒程序将其杀掉。	研究创新型	必做

五、实验教材（指导书）或网络资源

- [1] 卓新建. 计算机病毒原理及防治. 北京：北京邮电大学出版社，2004.
- [2] 王路群. 计算机病毒原理及防范技术. 北京：中国水利水电出版社，2009.

六、考核方式

主要考察现场情况，包括以下几项：

- (1) 学习态度（实验室内是否有违纪情况）与实践动手能力（独立分析与解决问题）（10分）
- (2) 课题完成情况（功能完善）（10分）
- (3) 演示情况（运行稳定、界面友好）（10分）

网络攻防实验实验教学大纲

一、实验基本信息

课程编号：201421305

中文名称：网络攻防实验

英文名称：Network Attack and Defense Experiments

课程性质：专业选修课程

面向专业：信息安全（保密技术）

开设学期：7

课程总学时：24

实验学时：24

是否独立设课：是

二、实验目的和任务

网络攻防实验是信息安全专业的重要专业选修课程之一，旨在了解和掌握网络环境下攻击和防御的原理、技术和实际操作过程，培养学生对网络攻防的深度理解，从而具备网络攻击防御的方法技术。

三、实验教学基本要求

(1) 系统的了解主流的网络攻击与防御技术；

(2) 根据网络安全所面临的不同威胁，掌握信息收集、口令攻击、缓冲区溢出、恶意代码、Web应用程序攻击、嗅探、假消息、拒绝服务攻击等多种攻击技术；

(3) 从网络安全、访问控制机制、防火墙技术、入侵检测、蜜罐技术等方面掌握网络安全防御技术，进而掌握内网安全管理的技术和手段。

四、实验项目基本情况

序号	实验项目名称	实验学时	内容提要	实验类型	实验要求	备注
1	网络信息收集	4	掌握网络踩点、网络扫描和网络查点的基本原则和步骤，针对特定目标设计并实现信息收集	基本型	必做	
2	网络嗅探与协议分析	4	掌握网络嗅探、网络协议分析的基本步骤和原理，利用网络协议分析	基本型	必做	

			工具 Wireshark 实现嗅探和分析			
3	TCP/IP 网络协议攻击	4	掌握 TCP/IP 网络协议栈安全原理, 设计和实现网络层协议攻击、传输层协议攻击。设计和实现 TCP/IP 网络协议栈攻击防范实验	基本型	必做	
4	Windows 操作系统安全攻防	4	掌握 Windows 操作系统的安全体系结构与机制, 实现 Windows 远程安全攻防和本地攻防实验	综合设计型	必做	
5	Linux 操作系统安全攻防	4	掌握 Linux 操作系统安全机制, 设计并实现 Linux 系统远程攻防和本地攻防实验	综合设计型	必做	
6	Web 安全攻防技术与实践	4	掌握 Web 应用程序体系结构及其安全威胁, 掌握 Web 应用安全攻防技术, 设计实现 SQL 注入和 XSS 跨站脚本攻击实验	综合设计型	必做	

五、实验教材（指导书）或网络资源

- [1] 诸葛建伟. 网络攻防技术与实践. 电子工业出版社, 2011
- [2] 福罗赞(Behrouz A.Forouzan)、谢希仁. TCP/IP 协议族(第 4 版), 清华大学出版社 2011
- [3] 雅各布森(Douglas Jacobson)、仰礼友. 网络安全基础: 网络攻防、协议与安全. 电子工业出版社, 2011

六、考核方式

教学基本要求项	考核形式	占总成绩的比例
实验过程是否符合要求, 实验结果是否正确无误。	根据实验目标的实际完成情况	60%
实验报告是否符合报告文档的基本要求, 包括规范程度、完整程度	实验报告	40%