【计算机信息安全】

【Computer Information Security】

一、基本信息（必填项）

课程代码：【2050066】
课程学分：【4】
面向专业：【网络工程】
课程性质：【院级专业必修课】
开课院系：【信息技术学院网络工程系】
使用教材：主教材【网络安全技术及应用（第 2 版）贾铁军主编 机械工业出版社 2014 年 9 月】
（“十三五”国家重点出版规划项目，上海高校优秀教材奖，上海高校精品课程教材）
辅助教材【网络安全技术及应用实践教程（第 2 版）贾铁军主编 机械工业出版社 2016 年 1 月】
参考教材【计算机信息安全技术 付永钢 清华大学出版社 2016 年 2 月（信息安全专业用）】
参考网站【上海市高校精品课程“网络安全技术”资源网站：http://jiatj.sdju.edu.cn/webanq/ 】
先修课程：【计算机网络 0050064】、【操作系统 2050220】、【数据库原理 2050217】、【程序设计】

二、课程简介（必填项）

本课程是计算机类学科网络工程专业与专业特色课程，是网络工程专业必备的理论联系实践、融会贯通所学专业知识的综合性课程。随着信息技术的发展与应用，网络信息安全的内涵在不断的延伸，从最初的信息保密性发展到信息的完整性、可用性、可控性和不可否认性，进而又发展为“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等多方面的基础理论和实施技术。

通过本课程的学习，使学生理解计算机网络安全的基本知识、原理及其应用技术，主要包括：计算机网络安全概述和基本安全问题；网络安全技术的基本概念、内容和方法；网络协议安全、安全体系结构、网络安全管理技术、安全服务与安全机制、无线网安全技术及应用；入侵检测技术、黑客的攻击与防范技术；身份认证与访问控制技术；网络安全中的密码与压缩技术；病毒及恶意软件的防护技术；防火墙技术及应用；操作系统与站点安全技术、数据与数据库安全技术；电子商务网站安全技术及应用等。

三、选课建议（必填项）

“计算机信息安全”课程适合计算机类网络工程等专业的学生必修，除了学过计算机网络、数据库原理等课程之外，这些学生已掌握 1-2 门程序设计语言，从而具备了学好该课程的综合应用能力和基本必要的知识。提高学生对网络信息安全问题的分析、综合、实践和创新能力，“教、学、做、练、用一体化”，，使学生能够融会贯通掌握所学知识、技术和方法，为未来就业打好基础。建议本课程采用案例驱动的教学方式，通过大量的安全实例，不仅提高学生的网络安全意识，同时通过实验提高学生动手能力，使得学生能够较好地胜任后续课程的学习以及工作。

四、课程与培养学生能力的关联性（必填项）

自主学习	表达沟通	专业能力					尽责抗压	协同创新	服务关爱	信息应用	国际视野
		软件开发	系统运维	网络工程设计与实施	网络安全管理	网络协议分析					
●	●	●	●	●	●	●	●	●	●	●	●

注：教学大纲电子版公布在本学院课程网站上，并发送到教务处存档。

五、课程学习目标（必填项）

本课程以培养学生应用“网络信息安全”的主要技能和综合应用的职业素养为主线，“教、学、做、练、用一体化”，围绕计算机及手机终端设备网络信息安全的现状、常用关键技术和实际应用、解决方案的需求分析设计与实现等内容展开，使学生能够融会贯通掌握所学知识、技术和方法，为未来就业打好基础。建议本课程采用案例驱动的教学方式，通过大量的安全实例，不仅提高学生的网络安全意识，同时通过实验提高学生动手能力，使得学生能够较好地胜任后续课程的学习以及工作。。

知识目标：培养掌握计算机网络信息安全的现状、常用关键技术和实际应用、解决方案的需求分析设计与实现等内容展开，使学生能够融会贯通掌握所学知识、技术和方法，为未来就业打好基础。

能力目标：培养学生掌握常用关键技术和实际应用的能力和实际动手能力；利用信息安全技术对企事业网络信息安全解决方案的需求分析、设计与实现的分析解决问题的能力。

情感目标：通过“模拟企业项目推进法”，培养学生团队合作能力。

六、课程内容（必填项）

第 1 章　网络安全概述

通过本章学习，学生可以掌握网络安全的概念、特征、目标及内容；了解网络面临的威胁及其因素分析；掌握网络安全体系、网络安全模型和常用网络安全技术；了解实体安全技术的概念、内容、措施和隔离技术；理解构建设置虚拟局域网的同步实验

本章重点：网络安全的概念、特征、目标及内容；网络安全体系、模型和常用网络安全技术；

本章难点：网络安全体系和模型；构建设置虚拟局域网。

第 2 章　网络安全技术基础

通过本章学习，使学生了解网络协议的安全风险及新一代网络 Ipv6 的安全性；掌握虚拟专用网（VPN）技术特点及应用；掌握无线局域网（WLAN）安全技术及安全设置实验；掌握常用的网络安全管理工具及应用和方法。

本章重点：虚拟专用网（VPN）技术特点及应用；无线局域网（WLAN）安全技术和方法。

本章难点：网络协议的安全风险及新一代网络 Ipv6 的安全性。

第 3 章 网络安全管理概述

通过本章学习，学生可以掌握网络安全管理概念、任务、法律法规与取证、评估准则和方法；理解网络安全管理规范及策略、原则和制度；了解网络安全规划的主要内容和原则；掌握 Web 服务器的安全设置与管理实验。

本章重点：网络安全管理概念、任务、法律法规、评估准则和方法；管理规范及策略、原则和制度。

本章难点：网络安全规划的主要内容和原则；Web 服务器的安全设置与管理。

第 4 章　黑客攻防与检测防御

通过本章学习，学生可以较好地了解黑客攻击的目的及攻击步骤；熟悉黑客常用的攻击方法；理解防范黑客的措施；掌握黑客攻击过程，并防御黑客攻击；掌握入侵检测与防御系统的概念、功能、特点和应用方法。

本章重点：黑客常用的攻击方法、防范措施；入侵检测与防御系统的概念、功能、特点和应用。

本章难点：黑客常用的攻击方法、防范措施；入侵防御系统的概念、功能、特点和应用。

第 5 章　身份认证与访问控制

注：教学大纲电子版公布在本学院课程网站上，并发送到教务处存档。

通过本章学习，学生可以理解身份认证技术的概念、种类和常用方法；了解网络安全的登录认证与授权管理；掌握数字签名及访问控制技术及应用与实验；掌握安全审计技术及应用。

本章重点：身份认证技术的概念、种类和常用方法；数字签名及访问控制技术及应用。

本章难点：数字签名及访问控制技术及应用；安全审计技术及应用。

第 6 章　密码及加密技术

通过本章学习，学生可以较好地掌握密码技术相关概念、密码体制及加密方式；理解密码破译与密钥管理的常用方法；掌握实用加密技术、数据及网络加密方式；了解银行加密技术应用实例和加密技术；掌握常用 PGP 邮件加密应用实验。

本章重点：密码技术相关概念、密码体制及加密方式；密码破译与密钥管理的常用方法；实用加密技术、数据及网络加密方式；。

本章难点：密码体制及加密方式；密码破译与密钥管理的常用方法。

第 7 章　数据库安全技术

通过本章学习，学生可以掌握理解数据库安全的概念、面临的威胁及隐患;了解数据库安全的层次结构; 掌握数据库的安全特性、备份和恢复技术; 理解数据库的安全策略和机制、体系与防护、解决方案; 掌握SQL Server 2012用户安全管理实验。

本章重点：数据库安全的概念；数据库的安全特性、备份和恢复技术；

本章难点：数据库安全的层次结构;安全策略和机制、体系与防护、解决方案

第 8 章　计算机病毒防范

通过本章学习，学生能够较好地了解计算机病毒发展的历史和趋势；理解病毒的定义、分类、特征、结构、传播方式和病毒产生；掌握病毒检测、清除、防护、病毒和防病毒的发展趋势；掌握恶意软件概念、分类、防护和清除；掌握360安全卫士及杀毒软件应用实验。

本章重点：计算机病毒的定义、分类、特征、结构、传播方式和产生；掌握病毒检测、清除、防护。

本章难点：计算机病毒的特征、结构、传播方式和产生；掌握病毒检测、防护。

第 9 章　防火墙应用技术

通过本章学习，学生可以基本掌握防火墙的概念;防火墙的功能;了解防火墙的不同分类;掌握 SYN Flood 攻击的方式及用防火墙阻止其攻击的方法;掌握防火墙安全应用实验。

本章重点：防火墙的功能分类;SYN Flood攻击的方式及用防火墙阻止其攻击的方法。

本章难点：防火墙的功能分类;SYN Flood 攻击的方式及用防火墙阻止其攻击的方法。

第 10 章　操作系统及站点安全

通过本章学习，学生理解网络操作系统安全面临的威胁及脆弱性；掌握网络操作系统安全的概念和内容；掌握网络站点安全技术相关概念和内容；Windows Server 2012安全配置实验。

本章重点：网络操作系统安全的概念和内容；网络站点安全技术相关概念和内容。

本章难点：网络操作系统安全的概念和内容；网络站点安全技术相关概念和内容。

第 11 章　电子商务安全

通过本章学习，使学生了解电子商务安全的概念、安全威胁和风险；理解电子商务的SSL、SET 安全协议；掌握基于SSL 协议Web 服务器构建；理解移动电子商务的安全与无线公钥的安全体系WPKI 技术；掌握数字证书的获取与管理实验。

注：教学大纲电子版公布在本学院课程网站上，并发送到教务处存档。

本章重点：电子商务的SSL、SET 安全协议；基于SSL 协议Web 服务器构建。

本章难点：电子商务的SSL、SET 安全协议；基于SSL 协议Web 服务器构建。

第 12 章　网络安全解决方案

通过本章学习，学生了解网络安全方案概念和内容；理解安全方案目标及设计原则和质量标准；理解安全方案的需求分析和主要任务；掌握安全方案分析与设计、安全解决方案案例；掌握实施方案与技术支持、检测报告与方案编写。

本章重点：网络安全解决方案的需求分析和主要任务；方案分析与设计和实施。

本章难点：网络安全解决方案的需求分析、设计和实施。

七、课内实验名称及基本要求（适用于课内实验）

列出课程实验的名称、学时数、实验类型（演示型、验证型、设计型、综合型）及每个实验的内容简述。

序号	实验名称	主要内容	实验时数	实验类型	备注
1	构建设置虚拟局域网	选定一种虚拟机应用软件，确定系统的功能、特点和应用范围，构建并设置虚拟局域网。	2	设计型	计算机网络信息安全攻防实验准备工作
2	无线局域网（WLAN）安全设置实验	无线局域网（WLAN）安全的设置要求、方法、步骤并检验。	2	验证型	
3	Web 服务器的安全设置与管理	Web 服务器的安全设置与管理方式、方法、步骤	2	验证型	
4	网络系统扫描及检测实验	网络系统扫描及检测工具、方式、方法、步骤和效果	4	综合型	
5	网银登录、身份认证及数字签名实验	网银登录、身份认证、访问控制及数字签名的方式、方法、步骤	2	综合型	
6	常用 PGP 邮件加密应用实验	常用 PGP 邮件加密软件下载、应用方式、方法、步骤	2	验证型	
7	SQL Server 2012 用户安全设置（或数据备份恢复实验）	SQL Server 2012 用户安全设置（或数据备份恢复实验）	2(二选一)	验证型	
8	360 安全卫士杀毒软件应用实验	360 安全卫士杀毒软件应用	2	验证型	

注：教学大纲电子版公布在本学院课程网站上，并发送到教务处存档。

9	防火墙安全应用实验	防火墙安全应用实验要求、安装及设置方法、步骤	4	综合型	
10	Windows Server 2012 安全配置实验	Windows Server 2012 安全配置实验	2	验证型	
11	网购支付数字证书的获取与管理实验	网购支付数字证书的获取与管理实验	2	综合型	
12	网络安全解决方案的需求分析、设计和实施	网络安全解决方案的需求分析、设计和实施	4	设计型	任务分组到人，分工合作，交流分析设计及实施（解决方案）

注：共 32 学时，复习和机动 2 学时（“十一”等放假）。

八、评价方式与成绩（必填项）

总评构成（1+X）	（1）	（X）		
评价方式	期末考核 开卷笔试	（X1） 出勤及课堂表现（20%）	（X2） 分组交流讨论（20%）	（X3） 作业和实验报告（20%）
1 与 X 两项所占比例%	40%	60%		

“1”一般为总结性评价，“X”为过程性评价，“X”的次数一般不少于 3 次，无论是“1”、还是“X”，都可以是纸笔测试，也可以是表现性评价。与能力本位相适应的课程评价方式，较少采用纸笔测试，较多采用表现性评价。

常用的评价方式有：课堂展示、口头报告、论文、日志、反思、调查报告、个人项目报告、小组项目报告、实验报告、读书报告、作品（选集）、口试、课堂小测验、期终闭卷考、期终开卷考、工作现场评估、自我评估、同辈评估等等。

本大纲只对“1”的考核方式以及比例进行规定，对“X”不予规定，由任课教师自行决定 X 的内容、次数及比例，同一门课程由多个教师共同授课的、由课程组共同讨论决定 X 的内容、次数及比例。

撰写：贾铁军　　系主任审核：巢爱棠　　院长签字：徐方勤

2016.6.28

注：教学大纲电子版公布在本学院课程网站上，并发送到教务处存档。