《网络空间与安全技术》教学大纲

课程编号：071233A

课程类型：□通识教育必修课 □通识教育选修课

□学科基础课 ☑专业核心课

□专业提升课 □专业拓展课

总 学 时：48 讲课学时：32 实验（上机）学时：16

学　　分：3

考试类型： ☑考试 □考查

适用对象：计算机科学与技术专业

☑是 □否 适合作为其他专业学生的个性化选修课

先修课程：计算机基础、程序设计、数据库原理、操作系统、计算机网络等

一、教学目标

本课程是计算机科学与技术专业的专业核心课程，是为适应信息社会对网络空间安全管理和应用人才要求而开设的。既重视学生相关理论的系统学习，又强调培养学生发现问题、分析问题和解决问题的实践能力，在信息技术及网络空间安全等领域的人才培养方面发挥不可替代的重要作用。

网络空间安全涉及方方面面，既包括网络自身及其所承载的信息和业务应用安全，也包括由网络空间衍生出的社会性安全问题。总体来说，本课程分为三大方面的内容：网络空间安全威胁和管理、网络空间安全技术以及网络空间安全研究热点。通过本课程的学习，将达到以下教学目标。

目标1：通过系统的介绍网络空间安全概念、理论以及网络空间安全威胁及管理政策，使学生对网络空间安全有一个整体的认识；

目标2：了解网络空间不安全的各种因素，理解实现网络安全的重要性；掌握网络空间安全的防御技术和方法

目标3：理解当前世界网络空间安全的研究热点及相关技术

最终使学生具备从事网络系统安全设计和网络系统安全管理所需要的基础知识和专业技能，使学生毕业后能够迅速参与网络系统空间安全研究、设计与管理的实际工作。

课程思政教学目标：注重在网络安全应用技术等方面的正确引导，培养学生具备网络空间安全的意识以及掌握常用的网络安全技术。将相关法律法规、职业素养以及专业使命等融入课程，让学生认识到国家利益与网络空间安全的关系，将国家发展与自我定位相结合，增强学生在网络空间中的法律常识，帮助其树立正确的网络道德观，并鼓励学生努力学习先进科学技术，服务国家、回馈社会。

二、教学内容及其与毕业要求的对应关系

可包括但不限于：

1、教学内容

本课程是一门理论性、实践性并重的专业课程，课程内容几乎涵盖了网络空间安全领域的方方面面，因而课程教学难度大。为了能够在有限的48学时内掌握关键的安全技术，具备初步规划企业基本安全方案的能力，在教学中，授课内容应从多种教材和网络媒介归纳综合；要侧重从总体知识体系的层面介绍网络空间安全的概念、原理、威胁及管理政策；重点介绍网络空间安全的攻击技术和防御技术，使学生掌握如何运用这些技术构建网络空间的安全体系；要以当前的主流技术思想和实践为主，同时结合网络安全领域的最新研究成果和解决方案，对网络安全软件应用、企业及个人网络安全等专题进行研究和讨论。

（1）知识体系

第一部分：网络空间安全概述，包括网络空间安全的基本概念、网络空间安全面临的威胁、网络安全体系结构、网络安全管理；

第二部分：网络攻击手段，包括黑客的基本概念、网络入侵过程、常用的网络攻击手段；

第三部分：网络空间安全技术，包括网络安全架构/分层，通用安全技术（如认证与加密技术、身份管理等）、网络层安全技术及策略（如信息隔离与防火墙技术、入侵检测技术等）、通用基础系统安全（如操作系统安全技术、数据库安全技术、备份与恢复技术等）、业务应用安全（如安全审计、访问控制技术等）以及信息内容安全（垃圾信息防范、内容识别与过滤）等。

第四部分：网络空间安全研究热点，包括移动互联网安全、云计算机安全、下一代互联网安全、大数据安全等安全风险及相关研究思考。

第五部分：网络安全解决方案，包括网络安全解决方案的基本概念、网络安全解决方案的基本框架。

（2）核心内容介绍

本课程的核心内容包括网络空间安全攻击与防御技术，即知识体系中第二部分与第三部分。

2、教学方法与手段

根据教学目标，拟采用的教学方法有：课堂讲解基本概念和核心知识，讲授和讨论相结合领会知识要点，案例教学训练解决问题的能力，借助网络安全实验教学辅助系统和PGP、Snot、Sniffer、EasyRecovery、SupperScan、SSS、LC5等多种软件工具进行上机操作和具体实践。

3、实践教学环节

本课程有大量的内容需要借助于网络安全实验教学辅助系统和PGP、Snot、Sniffer、EasyRecovery、SupperScan、SSS、LC5等多种软件工具进行学习，建议自学时安装相关软件进行自学（教师应提示学生安装哪些软件）。通过上机学习本课程的理论，掌握网络安全防御的技术与方法。

4、课后作业及自学要求

为有效学习本课程，要求学生首先具备计算机基础、计算机系统、程序设计等方面的基础知识，具备计算机网络及通信、数据库原理、操作系统、信息系统分析与设计等专业知识。

自学时应该熟读大纲，提纲挈领地掌握网络安全技术的内容，随后，按照大纲熟读教材，还要参考大量的参考文献，通过课后思考和练习题进行多角度和层次的反复学习。

5、与毕业要求的对应关系

通过本课程的学习学生能够系统地掌握网络空间安全基本理论及安全防御技术，具备利用现代化工具解决实际网络安全工程项目的应用分析能力，具备网络安全从业人员的专业素质和职业道德规范。毕业后能够迅速参与到网络系统空间安全研究、设计与管理的实际工作中去。

6、教学中其它需要说明的问题

课程学时较少，教师可根据实际情况选择授课内容和实践内容。

三、各教学环节学时分配

以表格方式表现各章节的学时分配，表格如下：

**教学课时分配**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 章节内容 | 讲课 | 实验 | 其他 | 合计 |
| **1** | 第1章 网络空间安全概述 | **3** | **2** |  | **5** |
| **2** | 第2章 网络攻击与防范 | **6** | **2** |  | **8** |
| **3** | 第3章 通用安全技术 | **6** | **4** |  | **10** |
| **4** | 第4章 网络层安全技术 | **8** | **4** |  | **12** |
| **5** | 第5章 通用系统/平台安全技术 | **3** | **2** |  | **5** |
| **6** | 第6章 计算机病毒防范技术 | **2** | **2** |  | **4** |
| **7** | 第7章 信息内容安全技术 | **2** |  |  | **2** |
| **8** | 第8章 网络空间安全研究热点 | **2** |  |  | **2** |
| **合计** |  | **32** | **16** |  | **48** |

四、教学内容

第1章 网络空间安全概述

第一节 “网络空间”及网络空间安全

1.网络空间概念

2.网络空间安全概念及研究体系

3.研究网络空间安全的社会意义

第二节 网络空间安全威胁与热点事件分析

1.网络空间安全面临的主要威胁与挑战

2.近年来网络空间安全热点事件及分析

第三节 国内外网络空间安全状况及部署

1.中国网络空间安全状况及部署

2.美国网络空间安全状况及部署

3.俄罗斯网络空间安全状况及部署

4.英国网络空间安全状况及部署

第四节 网络空间安全管理和政策

1.政策规划战略

2.法律法规

3.国际合作与国际治理

教学重点和难点：

1.网络空间安全的研究体系。

2.研究网络空间安全的重要性和社会意义。

3.网络空间安全的基本概念及相关述语。

4.威胁网络空间安全的主要因素。

5.网络空间安全的法规及治理政策。

课程的考核要求：

了解：威胁网络空间安全的因素及来源。

理解：为什么要研究网络空间的安全问题。

掌握：网络空间安全的基本概念和相关术语，我国及国外网络空间安全部署及立法情况，网络空间安全蓝皮书的内容。

复习思考题：

1.网络空间安全的含义及目标是什么？

2.网络空间安全蓝皮书是什么？包括哪些内容？

3.国内和国际上对于网络空间安全方面的部署情况，网络空间安全的法规及治理政策有哪些？

4.为什么要研究网络空间安全？

课程思政切入点：

从国家主权高度认识网络空间安全与国家利益的关系，鼓励学生努力学习网络安全知识，主动承担护网责任，形成用网、爱网意识。

第2章 网络攻击与防范

第一节 黑客概念

1.黑客概念

2.黑客分类

3.黑客行为的发展趋势

第二节 网络攻击手段

1.网络扫描与网络监听

2.缓冲区溢出攻击

3.口令攻击

4.特洛伊木马

5.欺骗攻击

6.拒绝服务攻击

第三节 网络攻击过程

1.收集信息

2.确定攻击目标

3.探测系统安全弱点

4.攻击目标主机

5.销毁痕迹

第四节 网络空间安全防范技术

1.数据加密技术

2.网络信息安全扫描技术

3.防火墙技术

4.入侵检测技术

5.备份与恢复技术

6.计算机病毒防范技术

教学重点和难点：

1.网络攻击与网络安全的关系。

2.网络入侵的过程。

3.网络扫描和网络监听原理，拒绝服务攻击的概念及攻击原理，木马的工作原理。

课程考核的要求：

了解：黑客的概念及分类，黑客行为的发展趋势，黑客攻击的一般过程及网络防范技术。

理解：网络监听的原理，缓冲区溢出攻击的概念，网络空间安全防范技术的作用。

掌握：网络扫描工具的使用，口令攻击工具的使用，拒绝服务攻击的概念，特洛伊木马的概念及其工作原理。

应用：能够使用相关工具对目标主机进行相应操作。

复习思考题：

1.攻击者通常有几种？各自的含义是什么?

2.黑客对信息安全构成怎样的威胁?

3.黑客的攻击目的是什么?

4.简述黑客攻击的过程。

5.简述黑客攻击的常用手段,并作简单分析。

6.什么是特洛伊木马程序?

课程思政切入点：

通过对常见的网络攻击手段的讲解，提醒学生要注意上网安全,要小心网络社交,谨防网络诈骗,同时用好、管好自己的口令,并正确、安全地使用计算机。

第3章 通用安全技术

第一节 数据加密技术

1.数据加密的基本概念

2.常用加密机制

3.古典加密算法

4.DES加密算法

5.RSA加密算法

第二节 数字签名技术

1.数字签名的基本概念

2.数字签名的实现方法

第三节 公钥基础设施

1.PKI的基本概念

2.PKI的组成

3.PKI的功能

4.PKI的相关技术

5.我国PKI发展现状

教学重点和难点：

1.DES加密算法的概念及实现算法。

2.RSA加密算法的概念及实现算法。

3.PGP加密的原理和实现。

课程考核的要求：

了解：加密体系的种类及特点，DES解密技术的优缺点。

理解：密码学的基本概念。

掌握：RSA加密算法的基本原理，使用PGP加密工具进行文件和邮件的加密方法。

应用：依据古典和近代的密码算法设计并实现对指定字符的加密和解密。

复习思考题：

1.简述密码技术的概念?

2.列举古典加密方法,并对其做简要描述?

3.非对称加密算法RSA 主要特点是什么?

4.说明非对称加密算法实现数字签名过程。

第4章 网络层安全技术

第一节 防火墙的基本实现技术

1.包过滤技术

2.代理技术

3.状态监视技术

第二节 防火墙的基本结构

1.包过滤体系结构

2.屏蔽主机体系结构

3.屏蔽子网体系结构

第三节 防火墙的设置与选购

1.设置防火墙需要考虑的因素

2.防火墙的选购策略

第四节 入侵检测技术概述

1.入侵检测系统的基本概念

2.入侵检测系统与防火墙的关系

3.入侵检测系统与扫描器的关系

4.入侵检测的步骤

第五节 入侵检测技术简介

1.入侵检测系统的基本结构

2.入侵检测系统的类型

3.入侵检测系统的主要方法

第六节 入侵检测系统解决方案

1.入侵检测系统典型应用环境

2.入侵检测系统部署实例

3.入侵检测系统面临的挑战

教学重点和难点：

1.防火墙的基本概念及实现技术。

2.利用软件设置防火墙的规则。

3.防火墙的选购原则。

4.入侵检测的基本概念。

5.几种主流的入侵检测系统结构、特点和工作原理。

6.入侵检测系统的部署。

课程考核的要求：

了解：防火墙实现技术的原理，入侵检测的基本方法以及入侵检测的步骤。

理解：防火墙的基本概念和作用，入侵检测的基本概念。

掌握：防火墙过滤规则的设置方法，一种入侵检测系统的使用方法。

应用：能够使用防火墙软件工具创建简单防火墙规则的方法，能够针对实际的应用环境，通过使用入侵检测工具进行检测。

复习思考题：

1.简述防火墙的定义和作用?

2.试述包过滤防火墙技术的原理及特点?

3.试述代理防火墙技术的原理及特点。

4.常见的防火墙系统有哪几种？

5.设置防火墙需要考虑哪些因素？

6.双宿主堡垒主机与单宿主堡垒主机的区别是什么?

7.屏蔽子网的防火墙系统是如何实现的?

8.选购防火墙产品时有哪些注意事项?

9.什么是入侵检测系统?简述入侵检测系统面临的挑战。

10.简述入侵检测常用的方法。

11.简述入侵检测的步骤及每一步工作要点?

课程思政切入点：

结合我国已经颁布并实施的《中华人民共和国网络空间安全法》等相关法律法规及国内外案例，引导学生运用自身专业特长维护风清气正的网络空间安全环境，严格遵守网络安全法律法规，共建和谐网络环境。

第5章 通用系统/平台安全技术

第一节 访问控制技术

1.访问控制简介

2.自主访问控制

3.强制访问控制

第二节 操作系统安全技术

1.操作系统安全准则

2.操作系统安全的防护方法

3.操作系统资源防护技术

4.Windows操作系统安全防护方案

第三节 数据库安全技术

1.数据库的安全问题

2.数据库的安全需求

3.数据库管理系统的安全措施

第四节 数据备份与恢复

1.数据备份

2.数据恢复

教学重点和难点：

1.访问控制技术的概念及种类，访问控制的实现技术及方法。

2.备份的概念及内容，恢复应注意的问题。

3.操作系统安全防护的方法及措施。

课程考核的要求：

了解：访问控制技术及其实现技术，备份的概念。

理解：操作系统安全防护的基本需求。

掌握：恢复时应注意的问题，常用操作系统安全防护的方法。

应用：根据实际计算机系统环境配置安全的操作系统。

复习思考题：

1.简述操作系统帐号管理的重要性。

2.有几种方法可以保护密码不被破解或被盗取?

3.简述审核策略、密码策略和帐户策略的含义。

4.简述审核、密码和帐户等策略如何保护操作系统不被入侵？

5.如何关闭不需要的端和服务？

第6章 计算机病毒与防范技术

第一节 计算机病毒概述

1.计算机病毒的定义

2.计算机病毒的特征

3.计算机病毒的类型

4.计算机病毒的结构

第二节 计算机病毒的工作原理

1.计算机病毒的引导过程

2.计算机病毒的触发机制

3.计算机病毒的传播

第三节 感染病毒后计算机系统的症状

1.计算机病毒发作前的症状

2.计算机病毒发作时的症状

3.计算机病毒发作后的症状

第四节 典型的计算机病毒分析

第五节 计算机病毒的防治方法

1.计算机病毒的清除

2.感染病毒后的修复措施

3.计算机病毒的防范方法

教学重点和难点：

1.病毒的概念及种类。

2.病毒的检测及消除。

3.病毒的防范。

课程考核的要求：

了解：病毒的基本概念。

理解：病毒的工作原理。

掌握：病毒的检测及消除方法，病毒的防范措施。

应用：防病毒软件的使用。

复习思考题：

1.什么是计算机病毒? 它有哪些危害?

2.计算机病毒的特征有哪些?

3.如何清除和预防计算机病毒?

第7章 信息内容安全技术

第一节 数字水印

1.概述

2.数字水印原理及分类

3.数字水印的关键技术

4.数字水印的攻击与测试

第二节 数字版权管理

1.定义与原理

2.数字版权管理技术

3.应用场景

4.案例

第三节 信息过滤

1.信息过滤原理

2.信息过滤分类体系

3.信息过滤技术与实现方式

4.信息内容特征识别

5.信息过滤结果评价

教学重点和难点：

1.数字版权管理技术。

2.信息过滤技术与实现方式。

3.数字水印关键技术。

课程考核的要求：

了解：数字水印、数字版权、信息过滤的基本概念。

理解：信息过滤分类。

掌握：数字水印、数字版权、信息过滤的关键技术。

应用：信息内容安全技术的使用。

复习思考题：

1.什么是数字水印？数字水印攻击有哪些情形？

2.数字版权管理技术有哪些?

3.信息内容过滤方式有哪些?

课程思政切入点：

从2014年开始，每年九月份都会开展“国家网络安全宣传周”主题活动，鼓励学生了解并参与每年的网络安全宣传周，体验网络安全活动，观看相关专题片视频，了解网络安全的内涵与外延，激发学生学习兴趣。

第8章 网络空间安全研究热点

第一节 移动互联网安全

1.智能终端安全

2.无线局域网安全

3.移动应用安全

第二节 云计算安全

1.云计算安全的关键技术

2.云计算面临的安全风险

3.国内外云服务安全现状与挑战

4.云安全的主要研究方向

第三节 下一代互联网安全

1.下一代互联网的定义和特征

2.下一代互联网的安全现状

3.下一代互联网的安全隐患及对策

4.下一代互联网的安全展望

第四节 大数据安全

1.大数据安全概述

2.大数据安全风险

3.国内外大数据安全政策措施

4.大数据安全关键技术及应对

课程思政切入点：

每年网络空间安全课程都会通过结合近一年来社会上发生的热点网络安全事件（如酒店客户数据外泄、电网、工业互联网遭受攻击、App应用恶意软件等），使学生从内心真正体会网络安全的重要性，触动学生在网络安全学习中体会网络安全上升为国家战略的含义以及学习网络安全的专业使命。

五、考核方式、成绩评定

本课程的考核分为平时考核及期末考核两种形式。本课程平时成绩占40%，期末考试成绩占60%。

平时考核采用课下调研撰写报告、课堂案例讨论和上机操作实验等方式。

平时成绩的分配比例为：考勤占10%，调研报告成绩占5%，课堂案例讨论成绩占5%、上机操作实验等成绩占20%。

期末考核采用闭卷形式，试题内容要注重知识应用能力和解决问题能力的考核上，而知识点的记忆和理解要服务于学生能力的提高和巩固。

六、主要参考书及其他内容

1．梁亚声等编著.计算机网络安全教程（第三版）.北京：机械工业出版社.2018.2

2．刘建伟，王育民编著. 网络安全技术与实践.北京：清华大学出版社.2011.6

3．陈志德等编著. 网络安全理论与应用.北京：电子工业出版社.2012.6

4．张世永编著. 网络安全原理与应用.北京：科学出版社.2012.12

5．Mark Stamp编著，张戈 译. 信息安全原理与实践.北京：清华大学出版社.2013.5

6.魏亮，魏薇等编著.网络空间安全.北京：电子工业出版社.2016.1

执笔人：周晓磊 教研室主任：高静 系教学主任审核签名：