**《信息安全课程设计》课程教学大纲**

执笔人：张致远 修订日期：2022年11月

**一、课程基本信息**

1．课程编号：P401141B

2．课程平台：创新实践平台

3．课程模块：综合实践模块

4．课程性质：选修

5．学时/学分：32/1

6．先修课程：信息安全理论基础（A）

7．适用专业：信息工程

8．教学单位名称：电信学院网络与安全教学团队

**二、课程教学目标**

**课程目标1**. 通过信息安全相关的实验设计及案例分析，使学生掌握信息安全相关的理论、原理，能够运用基本原理和方法，分析和设计信息及信息系统和信息网络的安全机制。

**课程目标2.** 培养学生对信息安全问题和信息安全技术的正确认识，培养正确的思考方法，建立社会责任与社会服务意识。

**三、课程目标和毕业要求的对应关系**

|  |  |  |
| --- | --- | --- |
| **毕业要求** | **毕业要求指标点** | **课程目标** |
| 2. 工程知识：能够应用数学、自然科学、工程基础和专业知识的基本原理，将信息复杂工程问题抽象为数学、物理问题，选择适当的模型进行描述，对模型进行分析求解。 | 2.4将数学、自然科学、工程基础和专业知识用于工程问题的计算分析。 | 1，2 |
| 4. 设计/开发解决方案：能够综合考虑经济、社会、健康、安全、法律、文化及环境因素，针对信息复杂工程问题设计有效的解决方案，按照具体需求实现信息工程系统或模块，在此过程中能够体现创新意识，并对设计方案进行测试与改进。 | 4.3 对设计系统进行功能和性能测试，进行必要的方案改进。 | 1，2 |
| 9. 职业规范：具有人文社会科学素养，具有社会主义核心价值观和社会责任感，能够在工程实践中理解并遵守工程职业道德和规范，履行责任。 | 9.1 具备人文社会科学素养，理解应担负的社会责任，愿意为社会服务。 | 2 |

**四、课程思政育人目标**

**目标1.** 介绍课程技术发展史，特别是有关方面的国家重大科技成果，让学生们树立正确理想信念，服务于国家重大战略。

**目标2.** 介绍课程中科技工作者的成就和贡献，培养学生严谨务实的治学精神和探索精神。

**目标3.** 引入研究型教学，配合思政案例，启发辩证思维，培养学生工匠精神，提高学生动手实践能力。

**五、课程教学内容和要求**

**课程主要知识点、重点、难点及课时分配**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **知识单元（章节）** | **知识点** | **教学要求** | **推荐学时** | **教学方式** | **支撑课程目标** |
| 1 | 设计任务布置 | 讲解课程设计的任务、任务选择和学生分组 | 1. 回顾信息安全理论基础各章重点内容及知识点 2. 根据重点难点问题选择合适的题目 3. 分组进行任务的设计实现 | 2 | 讲授 | 1 |
| 2 | 课程设计 | TCP端口扫描工具的设计与实现 | 1. 深入了解TCP的连接建立过程； 2. 学习端口扫描技术，比较、分析不同的技术的特点； 3. 设计实现一个能够对TCP端口进行自动扫描的工具； 4. 可以指定端口范围、IP地址范围，并返回扫描结果。 | 26 | 讲授 | 1 |
| 端到端加密的即时通讯软件设计与实现 | 1. 选择或设计一种消息加密算法； 2. 设计一种密钥交换或分发机制； 3. 设计一个可以对消息进行加密/解密的即时通信软件； 4. 对即时通信软件进行实现。 | 讲授 | 1 |
| 基于AES对称密码体系的加密解密工具实现 | 1. 深入了解对称密码体系的工作方式，分析各种对称加密方法的特点、安全强度及弱点； 2. 详细说明AES算法的原理与结构； 3. 设计并实现一个可以对字符串、文本文件、二进制文件进行加密和解密的工具； 4. 工具支持128bit和256bit两种长度的密钥。 | 讲授 | 1 |
| 基于RSA非对称密码体系的加密解密工具实现 | 1. 深入了解非对称密码体系的工作方式，分析各种非对称加密方法的特点、安全强度及弱点； 2. 详细说明RSA算法的原理与结构； 3. 设计并实现一个可以产生非对称密钥并对字符串、文本文件、二进制文件进行加密和解密的工具； 4. 工具支持1024bit的密钥长度。 | 讲授 | 1 |
| 局域网侦听软件设计  与实现 | 1. 深入了解局域网的工作方式，研究局域网侦听技术，以及侦听探测技术； 2. 设计能够对局域网内的通信进行侦听的软件； 3. 能够解析侦听到的局域网通信（链路层、网络层）； 4. 编程实现并测试所设计的工具。 | 讲授 | 1 |
| 基于SHA1算法的摘要工具的设计与实现 | 1. 学习消息摘要算法的基本理论，分析各种摘要算法的优缺点； 2. 详细了解SHA1算法的计算过程； 3. 设计一个能够实现SHA1算法的摘要工具； 4. 编程实现所设计的工具，并能够对字符串、文件进行摘要，对摘要进行验证。 | 讲授 | 2 |
| DOS攻击检测及防御方法研究 | 1. 学习网络攻击的各种方式以及防御攻击的方法； 2. 深入了解DOS攻击的基本原理、攻击方式的种类等； 3. 设计并实现检测DOS攻击的工具，并进行验证； 4. 研究防御DOS攻击的方法，并加以实现。 | 讲授 | 2 |
| SSH客户端的设计与实现 | 1. 深入了解SSH的工作原理和工作方式； 2. 详细设计一个SSH客户端软件； 3. 编程实现所设计的软件； 4. 连接SSH服务器，验证所实现的软件。 | 讲授 | 2 |
| 10 | 报告及总结 | 课程设计报告、总结和讨论 | 能够对自己实现的任务从理论研究到功能实现能够进行完整的总结展示。 | 4 | 讲授 | 2 |

**五、课程教学安排**

本课是通信工程专业的专业课，需要灵活运用先修的信息、计算机网络通信、信息与网络安全等课程的基础理论知识，解决实际的工程问题，并设计和检验具体的解决方案。课程涉及到先前和后续专业课程的多个领域，适宜采用灵活多样的教学方式，将工程设计、研讨、自主学习等有机结合。通过课程设计过程中的答疑，指导学生培养自学和知识拓展能力，培养运用工具解决复杂系统问题的能力。

**1．课程设计题目设置**

本课程应根据信息和网络安全中的基本知识点、安全问题发展趋势等，在课程前期设计相应的课程设计题目。题目应具有综合性和明确的目的性，使学生需要综合利用各类知识和工具，完成设计，并进行结果验证。本课程强调解决复杂实际问题的设计能力，题目设置应具有一定的开放性，为学生提供知识拓展的空间。

**2．题目分配**

本课程宜采用分组和组内多人合作完成的模式，题目分配中注意小组资源的均衡。课程设计的结果包括：设计报告和验证程序，其中设计报告包括题目背景、相关知识、问题分析、解决方案、结果及结果分析等内容。

**4．课程思政**

本课程与信息安全和网络安全的日常问题息息相关，课程设计题目来自于实际网络通信环境。为了培养锻炼学生自学能力，对课程设计相关的实际安全问题，通过引入思政，结合相关课程内的理论知识，拓展并完善自己的知识体系和结构。

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 章节名称 | 知识点 | 所挖掘的思政元素 |
| 1 | 贯穿所有章节 | 网络安全内涵 | 【**树立国家总体安全观**】  习近平总书记在中央网络安全和信息化领导小组第一次会议上的讲话强调：没有网络安全就没有国家安全 |
| 2 | 密码学相关章节 | 对称、非对称加密工具实现 | 【**科学家品质-坚韧不拔探索-不折不挠专研】**  王小云教授几十年如一日，终于分析出了MD5算法 |
| 3 | 网络攻防相关章节 | 从主动攻击到被动防御 | 【**创新意识、主动探索**】  攻防是一对矛盾体，此消彼长，没有绝对的安全。希望同学们能够有通创新意识，迎难而上，解决各种难题 |

**六、课程的考核**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **课程成绩构成及比例** | **考核环节** | **目标分值** | **考核/评价细则** | **对应的课程目标** |
| 周报告 | 每周报告 | 30 | （1）主要考核小组的分工及进度安排的合理性；  （2）每周的报告5分，共6周。共30分. | 1 |
| 课程设计报告 | 课程设计报告文档，包括课程设计部分，研究部分 | 45 | 1. 考查学生自主学习、独立思考和拓展专业知识的能力。并且通过文字表达能力评价学生对解决问题的方案、系统设计和自主学习能力的掌握程度。 2. 教师根据课程设计的报告的完成情况评定成绩。满分45分 | 2 |
| 课程设计的程序及数值结果 | 带代码标注的课程设计程序文件及可执行文件 | 25 | （1）根据所完成的计算机程序及所得到的结果数据和数据分析进行成绩评定。  （2）程序质量、工作量、数据质量和数据分析的完善程度可作为衡量指标。 | 1 |

根据以上三项计算每名学生的总成绩，并将总成绩按照下表的转换方式，转换为五级11段的最终成绩：

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 百分制成绩 | 100-90 | 89-85 | 84-81 | 80-78 | 77-75 | 74-72 | 71-68 | 67-65 | 64-63 | 62-60 | 60以下 |
| 五级制成绩 | A | A- | B+ | B | B- | C+ | C | C- | D+ | D | F |
| 绩点 | 4.0 | 3.7 | 3.3 | 3 | 2.7 | 2.3 | 2.0 | 1.7 | 1.3 | 1.0 | 0 |

**七、本课程与其它课程的联系与分工**

先修课： 《信息安全理论基础》

后继课： 信息安全相关实践课程

**八、建议教材及教学参考书**

1. 蔡皖东 著，网络信息安全技术，北京，清华大学出版社，2015
2. 杜彦辉，信息安全技术教程，北京，清华大学出版社，2013
3. 安德森（Ross Anderson） 著；齐宁 等 译， 信息安全工程（第2版），北京，清华大学出版社，2012

**九、大纲审核人**

**十、学院审核程序说明**

由通信工程系制定，负责本科教学工作的系主任审核，经学院教学指导委员会审核批准。

**十一、学院审定日期**

**附：达成度评价方法：**

课程目标达成度评价包括课程分目标达成度评价和课程总目标达成度评价，具体计算方法如下：





课程目标评价内容及符号意义说明如附表1，字母*A*、*B*、*C*则分别表示周报告、课程设计报告、课程设计的程序及数值结果的实际得分

附表1 课程评价考核基本信息表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **课程目标评价内容** | **周报告** | **课程设计报告** | **课程设计程序及数值结果** | **课程总评成绩** |
| 目标分值 | 30 | 45 | 25 | 100 |
| 学生平均得分 | *A* | *B* | *C* | *A*+*B*+*C* |

课程目标达成度评价值计算具体说明如附表2。

附表2课程达成度评价计算方法

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **课程目标** | **考核环节** | **目标分值** | **学生平均得分** | **达成度计算示例** |
| 课程目标1 | 周报告 | 30 | *A* | 课程目标1达成度=（*A + C*）/ 55 |
| 课程设计程序及数值结果 | 25 | *C* |
| 课程目标2 | 课程设计报告 | 45 | *B* | 课程目标2达成度=*B* / 45 |
| 课程总体目标 | 总评成绩 | 100 | *A*+*B*+*C* | 课程总体目标 =*A*+*B*+*C*/ 100 |