# 《网络安全原理与实践》课程教学大纲

| | | | | | |
|---|---|---|---|---|---|
| 课程英文名 | **Network Security Principles and Practices** | | | | |
| 课程代码 | **B0501690** | 课程类别 | 学科专业课 | 课程性质 | 必修 |
| 学　分 | **3** | | 总学时数 | **48** | |
| 开课学院 | 计算机学院 | | 开课基层教学组织 | 网络与信息安全课程组 | |
| 面向专业 | 计算机科学与技术、智能财务(软件工程) | | 开课学期 | 第 6 学期 | |

**注：课程类别**是指学科基础课/专业课/实践环节/通识公共课/公共基础课/其他；

**课程性质**是指通识必修/通识选修/学科必修/专业必修/专业选修/实践必修/实践选修。

## 一、　课程目标

《网络安全原理与实践》是从事信息安全领域工作的入门课程，是计算机科学与技术专业的主要专业课，其目的是介绍网络安全基本理论与技术，包括网络攻击技术、网络安全编程、防火墙、恶意代码防护、VPN、无线网络安全技术以及网络安全协议等内容。通过本课程的学习，使学生初步掌握计算机网络安全的基本理论和基本方法，为进一步学习或从事信息安全领域的工作奠定必要的理论基础，结合国家网络安全战略和中华民族复兴的新时代背景，增强学生家国情怀与文化自信，激发学生使命感和责任心。

通过理论教学和实践活动，达到以下课程目标：

**课程目标 1**：能够基于网络安全基本原理知识，了解发展趋势及其对社会发展的影响。能够运用网络安全基本原理和专业知识，分析处理网络系统运行过程中遇到的实际问题。

**课程目标 2**：初步具备基本的网络安全功能原理、常用协议的分析能力；

**课程目标 3**：初步具备在真实网络条件下，设计组建计算机网络安全防护系统的能力；具备开发简单的计算机网络安全系统的能力。

**课程目标 4**：具有自主学习和终身学习意识及团队协作精神。

**课程目标 5**：具备客观辩证、探索创新等基本科学素养，及时了解网络安全的国内外新技术和发展趋势，了解国家在相关方面的网络安全战略需求，树立强烈的爱国主义使命感与责任心。

## 二、　课程目标与毕业要求对应关系

本课程的课程目标对计算机科学与技术专业毕业要求指标点的支撑情况如表 1 所示。

**表 1. 课程目标与计算机科学与技术专业毕业要求对应关系**

| 毕业要求 | 指标点 | 课程目标及支撑权重 |
|---|---|---|
| 毕业要求 1：工程知识：能够掌握数学、自然科 | 1-4 掌握计算机系统、物联网、 | 目标 1：0.4 |

| | | |
|---|---|---|
| 学、工程基础、计算机软件系统和计算机硬件体系知识，并应用在计算机相关领域的复杂工程问题的解决方案中。 | 人工智能、大数据、网络安全等某个专业领域的知识，并用于解决计算机领域的复杂工程问题。 | 目标 2：0.4<br>目标 3：0.2 |
| 毕业要求 3：设计/开发解决方案：能够设计计算机领域复杂工程问题的解决方案，设计与开发满足特定需求的软硬件系统、算法或部件，在设计中考虑社会、健康、安全、法律、文化以及环境等因素，并体现一定的创新意识。 | 3-4 能够在设计环节中体现创新意识。 | 目标 3：1.0 |
| 毕业要求 5：使用现代工具：能够针对复杂工程问题，开发、选择与使用恰当的技术、资源、现代工程工具和信息技术工具，包括对复杂工程问题的预测与模拟，并能够理解其局限性。 | 5-1：能够针对复杂工程问题，开发、选择与使用恰当的技术、资源、现代工程工具和信息技术工具 | 目标 2：0.5<br>目标 3：0.5 |
| 毕业要求 6：工程与社会：能够基于计算机工程相关背景知识进行合理分析、认识和评价计算机工程实践和复杂工程问题解决方案对社会、健康、安全、法律以及文化的影响，并理解应承担的责任。 | 6-1 能够基于计算机工程相关背景知识，合理分析与评价计算机工程实践和复杂工程问题解决方案对社会、健康、安全、法律及文化的影响。 | 目标 1：0.4<br>目标 2：0.4<br>目标 5：0.2 |
| 毕业要求 7：环境和可持续发展：了解国家信息产业发展的宏观政策，能够理解和评价计算机复杂工程问题解决方案及专业工程实践对环境、社会可持续发展的影响。 | 7-2 能够在计算机复杂工程问题解决方案中，考虑与环境、社会的和谐可持续发展。 | 目标 1：0.5<br>目标 5：0.5 |
| 毕业要求 12：终身学习：具有自主学习和终身学习的意识，有不断学习和适应信息技术高速发展的能力。 | 12-1：具有自主学习和终身学习的意识。 | 目标 4：1.0 |

本课程的课程目标对智能财务（软件工程）专业毕业要求指标点的支撑情况如表 2 所示。

**表 2. 课程目标与智能财务（软件工程）专业毕业要求对应关系**

| 毕业要求 | 指标点 | 课程目标及支撑权重 |
|---|---|---|
| 毕业要求 1：工程知识：能够掌握数学、自然科学、工程基础、计算机软件系统和计算机硬件体系知识，并应用在计算机相关领域的复杂工程问题的解决方案中。 | 1-4 掌握计算机系统、物联网、人工智能、大数据、网络安全等某个专业领域的知识，并用于解决计算机领域的复杂工程问题。 | 目标 1：0.4<br>目标 2：0.4<br>目标 3：0.2 |
| 毕业要求 3：设计/开发解决方案：能够设计计算机领域复杂工程问题的解决方案，设计与开发满足特定需求的软硬件系统、算法或部件，在设计中考虑社会、健康、安全、法律、文化以及环境等因素，并体现一定的创新意识。 | 3-4 能够在设计环节中体现创新意识。 | 目标 3：1.0 |
| 毕业要求 5：使用现代工具：能够针对复杂工程问题，开发、选择与使用恰当的技术、资源、现代工程工具和信息技术工具，包括对复杂工程问题的预测与模拟，并能够理解其局限性。 | 5-1：能够针对复杂工程问题，开发、选择与使用恰当的技术、资源、现代工程工具和信息技术工具 | 目标 2：0.5<br>目标 3：0.5 |

| | | |
|---|---|---|
| 毕业要求 6：工程与社会：能够基于计算机工程相关背景知识进行合理分析、认识和评价计算机工程实践和复杂工程问题解决方案对社会、健康、安全、法律以及文化的影响，并理解应承担的责任。 | 6-1 能够基于计算机工程相关背景知识，合理分析与评价计算机工程实践和复杂工程问题解决方案对社会、健康、安全、法律及文化的影响。 | 目标 1：0.4<br>目标 2：0.4<br>目标 5：0.2 |
| 毕业要求 7：环境和可持续发展：了解国家信息产业发展的宏观政策，能够理解和评价计算机复杂工程问题解决方案及专业工程实践对环境、社会可持续发展的影响。 | 7-2 能够在计算机复杂工程问题解决方案中，考虑与环境、社会的和谐可持续发展。 | 目标 1：0.5<br>目标 5：0.5 |
| 毕业要求 12：终身学习：具有自主学习和终身学习的意识，有不断学习和适应信息技术高速发展的能力。 | 12-1：具有自主学习和终身学习的意识。 | 目标 4：1.0 |

## 三、 课程目标与教学内容和方法的对应关系

**表 3. 课程目标与教学内容、教学方法的对应关系**

| 教学内容 | 教学方法 | 课程目标 |
|---|---|---|
| 1. 绪论 | 课堂讲授、视频学习、课堂讨论、课堂测试、文献查阅 | 1,2,4,5 |
| 2. 网络基础知识 | 课堂讲授、视频学习、课堂测试、案例分析 | 2,4,5 |
| 3. 网络安全基础编程 | 课堂讲授、视频学习、课堂讨论、课堂测试、案例分析、文献查阅 | 1,2,3,4,5 |
| 4. 网络攻击技术 | 课堂讲授、视频学习、课堂讨论、课堂测试、案例分析、文献查阅 | 1,2,3，4,5 |
| 5. 防火墙与入侵检测技术 | 课堂讲授、视频学习、PBL 教学法、课堂讨论、文献查阅 | 1,3，4 |
| 6. 恶意代码 | 课堂讲授、视频学习、PBL 教学法、课堂讨论、课堂测试、案例分析、文献查阅 | 1,2,3,4,5 |
| 7. 网络安全协议与 VPN | 课堂讲授、视频学习、课堂讨论、课堂测试、文献查阅 | 1,2,3,4 |
| 8. 安全操作系统基础 | 课堂讲授、视频学习、课堂讨论、文献查阅 | 1,4,5 |
| 9. 无线网络安全技术 | 课堂讲授、视频学习、PBL 教学法、课堂讨论、课堂测试、案例分析、文献查阅 | 2,3,4,5 |

本课程详细教学内容与方法阐述如下：

**1、绪论**

**（1）教学内容：**

- 信息安全的概念、内涵和外延；
- 信息安全威胁分类；
- 信息安全研究内容介绍；
- 现有信息安全服务
- 信息安全领域评估准则，以及相关信息安全法律；
- 信息安全问题与现状；

**（2）教学重点：**①信息安全的内涵和外延；②信息安全服务发挥的作用。

**（3）教学难点：**①信息安全威胁来源；②网络安全的体系结构。

**（4）教学要求：**学生能够掌握网络所面临的安全性威胁，清楚网络安全的研究内容以及目前所提供的安全服务。

**思政融合点 1：**引导学生查阅文献资料，学生课外能够通过网络搜集信息安全新闻、报道等方式加深对信息安全问题严重性的认识，了解我国信息安全领域所面临的挑战，激发学生的爱国主义热情、自豪感、使命感与忧患意识。

**2、网络基础知识**

**（1）教学内容：**

- 网络基础知识包括网络体系结构、网络协议及网络应用；
- 网络协议模型
- TCP，IP，UDP 等重要协议的包结构
- 网络命令和服务

**（2）教学重点：**①分析捕获数据包的协议结构；②网络命令。

**（3）教学难点：**①TC 协议包结构；②IP 协议包结构。

**（4）教学要求：**掌握网络协议模型，特别是 TCP/IP 模型和相关协议层的作用和划分； 掌握 TCP，UDP，IP，ICMP 等网络协议的包结构；分析已捕获的数据包的协议层结构； 掌握通过网络命令获取网络信息的使用方法；掌握网络服务如 web，ftp，email 等实现原理；了解网络协议在网络安全领域所处的位置

**思政融合点 2：**介绍中共中央成立网络安全和信息化领导小组的重要意义，让学生体会到网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，要从国际国内大势出发，总体布局，统筹各方，创新发展，努力把我国建设成为网络强国。

**3、网络安全基础编程**

**（1）教学内容：**

- 网络安全基础编程；
- 网络通信编程
- 扫描器编程
- 注册表安全编程
- 驻留程序编程
- 文件系统编程
- 定时程序编程
- 多线程编程

**（2）教学重点：**①区分网络通信编程使用的 socket，掌握一种 socket 编程实现网络通信；②掌握注册表读写操作以及运用网络安全知识进行注册表防护。

**（3）教学难点：**①综合使用文件系统，定时，驻留功能实现恶意代码程序的编写。

**（4）教学要求：**学生掌握网络 socket 通信编程、扫描器编程、注册表安全编程、恶意代码编程

实现技术、文件系统和驻留程序编程、多线程编程实现。

说明：本章主要讲解编程实现的例子程序，学生需结合实验进行编程练习,并实现创新性的程序设计。

**思政融合点 3：**引导学生学习《中华人民共和国网络安全法》，让学生了解其是我国规范网络空间安全管理方面问题的基础性法律，是依法治网、化解网络风险的法律重器，是让互联网在法治轨道上健康运行的重要保障。

**4、网络攻击技术**

**（1）教学内容：**

- 介绍黑客攻击的常用套路、方式、当前主流的攻击手段以及网络攻击技术的发展趋势；
- 信息搜集技术,攻击实施技术以及隐身巩固技术等典型技术原理和应用实现。

**（2）教学重点：**①扫描具体采用的技术原理。

**（3）教学难点：**①缓冲区溢出原理及具体实现。

**（4）教学要求：**学生掌握黑客攻击步骤；能够掌握信息搜集技术，包括踩点技术，扫描技术和监听技术原理与应用；掌握攻击实施技术，包括社会工程学攻击，漏洞攻击，溢出攻击，欺骗攻击等技术原理与实现；掌握隐身巩固技术，包括设置跳板，留后门，清除日志等具体实现原理；

说明：本章内容需要学生课外搜集有关当前具体攻击技术的实现原理以及危害性，以期获取最新攻击技术与趋势。

**思政融合点 4：**介绍窃听、重传、篡改、拒绝服务攻击、电子欺骗、非授权访问、病毒等常见安全问题，加强同学们的防范意识，了解基本的预防和检测技术。

**5、防火墙与入侵检测技术**

**（1）教学内容：**

- 防火墙的体系结构；
- 防火墙技术
- 入侵检测技术
- 防火墙的分组过滤技术
- 入侵检测的含义以及入侵检测数据分析技术
- 防火墙体系结构
- 入侵检测步骤

**（2）教学重点：**①分组过滤技术的技术原理，并制定包过滤规则集；②防火墙三种实现技术的优缺点和应用范围。

**（3）教学难点：**①入侵检测数据分析技术的实现原理。

**（4）教学要求：**学生掌握网络环境下防火墙的定义，内涵和作用；防火墙具体实现技术，包括分组过滤，状态检测和应用代理技术；防火墙体系结构，防火墙创建步骤；入侵检测技术定义与其在网络安全防护所起的作用；入侵检测数据分析技术，即检测理论，包括静态配置分析，异常检测，

误用检测；了解入侵检测步骤，现存缺陷和发展趋势；

**6、恶意代码**

**（1）教学内容：**

- 恶意代码实现机理；
- 破坏效果以及防护技术
- 病毒，木马，蠕虫具体实现机理
- 典型恶意代码如脚本病毒，pe 病毒，反弹木马，熊猫烧香蠕虫等的实现技术

**（2）教学重点：**①U 盘病毒代码实现；②PE 病毒代码实现。

**（3）教学难点：**①脚本病毒代码实现②恶意代码和病毒，木马，蠕虫之间的相互关系

**（4）教学要求：**学生掌握恶意代码的定义、一般实现机理； 能够进行恶意代码的分类，包括病毒，木马和蠕虫等技术的区别和相似性；学生能够掌握恶意代码的历史，现状以及发展趋势；能够确认辨别典型病毒，包括脚本病毒，宏病毒，PE 病毒，U 盘病毒等具体技术和代码实现；掌握木马原理，特点和具体分类；了解蠕虫技术原理、典型案例；

说明：

本章的内容涉及代码阅读理解，需要学生课外调试案例代码，并创新性的设计一款自己的恶意代码以及其查杀软件。

**7、网络安全协议与 VPN**

**（1）教学内容：**

- 网络安全协议 IPSEC，SSL 等；
- 应用 VPN 技术
- IPSEC 协议的应用模式，AH 和 ESP 协议的实现和包结构
- SSL 协议所处位置和协议实现应用
- VPN 技术应用场合和实现协议

**（2）教学重点：**①AH 协议和 ESP 协议的区别和具体实现。

**（3）教学难点：**①VPN 应用方式和协议实现

**（4）教学要求：**学生掌握 IPSEC 的 2 个子协议：AH 和 ESP、IPSEC 具体的实现方式，安全保护机制；学生能够了解 IPSEC 其他相关技术与概念，包括 SA，ISAKMP 等；掌握 SSL 协议具体实现的子协议，功能和安全保护机理；掌握 VPN 定义，分类，以及具体实现协议；

说明：

本章的内容相对理论较多，学生课外可以通过进行 VPN 的配置实践环节加深对此类协议的理解。

**8、安全操作系统基础**

**（1）教学内容：**

- 安全操作系统历史；
- 安全操作系统的基本理论知识

**（2）教学重点：**①理解主体、客体；②访问矩阵；③可信计算基；④安全内核。

**（3）教学难点：**①硬件安全机制；②最小特权管理；③访问控制；④可信通路；⑤安全审计。

**（4）教学要求：**学生了解安全操作系统历史，国内外现状； 学生掌握安全操作系统基本概念，包括主体，客体，访问矩阵，可信计算基，安全内核等；学生掌握安全操作系统基本理论，包括硬件安全机制，最小特权管理，访问控制，可信通路，安全审计等；学生了解 windows 操作系统安全保护实现原理，以及具体安全配置建议；

**思政融入点 5：**讲解操作系统的演化，通过华为鸿蒙系统相关安全等案例的讲解，使学生养成创新意识。

**9、无线网络安全技术**

**（1）教学内容：**

- 无线网络存在的安全威胁
- 无线局域网的安全协议
- 蓝牙技术
- 新一代移动网络的安全技术
- 无线网络安全领域所需的基本理论知识

**（2）教学重点：**①无线局域网的安全协议；②蓝牙技术。

**（3）教学难点：**①新一代移动网络的安全技术②无线网络安全协议之间的关系和区别

**（4）教学要求：**学生了解无线网络存在安全威胁、无线网络安全协议、新一代移动互联网存在的安全协议等；

**思政融入点 6：**讲解 3、4、5G 技术的发展，5G 被西方国家禁用的案例，从而引导学生科学与技术国界等的思考。

## 四、 实践环节及要求

参考配套的《网络安全原理与实践》实验指导手册完成实验。

## 五、 与其它课程的联系

**先修课程：**计算机网络

## 六、 学时分配

**表 4 学时分配表**

| 教 学 内 容 | 讲课时数 | 实验时数 | 实践学时 | 课内上机时数 | 课外上机时数 | 自学时数 | 习题课 | 讨论时数 |
|---|---|---|---|---|---|---|---|---|
| 绪论 | 3 | | | | | 2 | | |
| 网络基础知识 | 3 | 2 | | | 2 | 2 | | |
| 网络安全基础编程 | 3 | 2 | | | 2 | 2 | | |
| 网络攻击技术 | 6 | 2 | | | 2 | 1 | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 防火墙与入侵检测技术 | 3 | 2 | | | 2 | 1 | | |
| 恶意代码 | 3 | 2 | | | 2 | 1 | | |
| 网络安全协议与 VPN | 3 | 2 | | | 2 | 1 | | |
| 安全操作系统 | 3 | 2 | | | 2 | 1 | | |
| 无线网络安全技术 | 3 | 2 | | | 2 | 1 | | |
| 讨论课 | | | | | | | | 2 |
| **合　　计** | 30 | 16 | | | 16 | 12 | | 2 |
| **总　　计** | 48 计划学时+16 学时课外上机+12 自学学时 | | | | | | | |

备注：自学学时用于预习、复习、习题、自学、课堂拓展等学习活动等

## 七、　课程目标达成途径及学生成绩评定方法

### 1.课程目标达成途径

**表 5 课程目标与达成途径**

| 课程目标 | 达成途径 |
|---|---|
| **课程目标 1：**能够基于网络安全基本原理知识，了解发展趋势及其对社会发展的影响。能够运用网络安全基本原理和专业知识，分析处理网络系统运行过程中遇到的实际问题。 | 以引导式、启发式和总结式教学方法为主，通过重点/难点内容讲解、PBL 教学法、课后作业、布置学生文献查阅、进行随堂提问及课堂 ppt 演示等模式，帮助学生利用安全原理知识解决问题。 |
| **课程目标 2：**初步具备基本的网络安全功能原理、常用协议的分析能力； | 以启发式、分析式和研讨式教学方法为主，针对相关重点/难点内容，分组组织学生开展自主学习，通过课后作业、随堂提问及课堂讨论等模式，使学生具备基本的网络安全功能原理、常用协议的分析能力。 |
| **课程目标 3：**初步具备在真实网络条件下，设计组建计算机网络安全防护系统的能力；具备开发简单的计算机网络安全系统的能力 | 以分析式和研讨式教学方法为主，针对相关重点/难点内容，通过原理讲解、实际案例分析、PBL 教学法、课堂讨论、随堂提问等模式，使学生具备在真实网络条件下，设计组建计算机网络安全防护系统的能力。 |
| **课程目标 4：**具有自主学习和终身学习意识及团队协作精神。 | 通过个人基础实践保障学生能熟悉并掌握网络编程基本方法；通过团队综合实践，合作开发简单的网络应用系统，使学生具备开发简单的计算机网络安全系统的能力。<br>通过布置学生文献查阅、翻转课堂学习、课堂小组讨论、PBL 教学等模式，培养学生的自主学习能力、终身学习意识、团队协作精神。 |
| **课程目标 5：**具备客观辩证、探索创新等基本科学素养，及时了解网络安全的国内外新技术和发展趋势，了解国家在相关方面的网络安全战略需求，树立强烈的爱国主义使命感与责任心。 | 通过课堂讲授、课后自学、文献查阅、课堂讨论、PBL 教学法、总结报告等各种方式，让学生对计算机网络安全的现状与发展趋势有所了解，并进一步了解目前国内相关先进技术与取得的成就，从而建立强烈的民族自豪感与爱国主义使命感。 |

### 2.学生成绩评定方法

本课程为考试课程，考试方式为闭卷。课程采用形成性评价与终结性评价相结合的评价方法，学期总评成绩由两部分构成：采用线上/线下混合教学模式，建议平时成绩占比 50%、期末考试成绩占比 50%；采用传统教学模式（以教师讲授为准），建议平时成绩占比 40%、期末考试成绩占比 60%。平时成绩可包括（但不仅限于）课程思政实践、课后作业、视频学习、在线测试、在线讨论、课堂测试、课堂小组讨论、课堂报告演讲、课堂参与等项目，至少不少于 5 项。各部分的建议考核内容、在平时成绩中的建议比例、关联课程目标、在总成绩中的占比等，如表 6 所示，任课教师可根据实际授课情况调整。各考核内容的详细评分标准见表 7 所示。

**表 6. 课程考核与成绩评定方法**

| 考核项目 | 考核内容 | 关联的课程目标 | 占平时成绩比例 | 占总评成绩比重 |
|---|---|---|---|---|
| 平时成绩 | 课程思政实践 | 5 | 5-10% | 50% |
| | 课后作业 | 1,2,3 | 15%-20% | |
| | 课堂参与/小组讨论 | 1,2,3,4,5 | 10%-15% | |
| | 在线测试 | 1,4 | 15%-20% | |
| | 实验验收 | 1,3,4 | 10%-15% | |
| 期末考试 | 期末闭卷考试 | 1,2,3,4,5 | | 50% |
| 总评成绩 | | 1,2,3,4,5 | | 100% |

**表 7. 考核内容详细评分标准**

| 考核内容 | 评分标准 | | | |
|---|---|---|---|---|
| | 90-100 | 75-90 | 60-75 | ＜60 |
| 课程思政实践 | 报告条理清晰，文字流畅，字数≥4000，参考文献数量≥8 且相关性强；内容完整且材料丰富，体现强烈的使命感、责任心与民族自豪感 | 报告条理清楚，字数≥3000，参考文献数量≥5 且相关性较好；内容完整，材料不够丰富，能体现学生的使命感、责任心与民族自豪感 | 报告有一定条理，字数≥1000，参考文献数量≥2 且基本相关；内容基本完整但材料较少，能体现学生的使命感与民族自豪感 | 报告字数＜1000，参考文献数量＜2；内容少，或有抄袭现象，体现不出学生的使命感与民族自豪感 |
| 课后作业 | 非标作业：方案等设计合理，分析准确，能满足问题全部要求 | 非标讨论题：方案较合理，分析较正确，能基本满足问题全部要求 | 非标讨论题：方案基本合理，能满足问题大部分要求 | 非标讨论题：方案不够合理，只能满足问题少量要求 |
| | 标准题目：按照作业题目评分标准据实评价 | | | |
| 课堂参与 | 学习通测试、课堂练习、回答问题等据实评价；或参与回答次数在教学班前 15% | 学习通测试、课堂练习、回答问题等据实评价；或参与回答次数在教学班前 50% | 学习通测试、课堂练习、回答问题等据实评价；或参与回答次数在教学班前 85% | 学习通测试、课堂练习、回答问题等据实评价；或参与回答次数在教学班后 15% |
| 在线测试 | 客观题，在线课程系统按照评分标准自动据实评价 | | | |
| 小组讨论 | 非标讨论题：小组方案合理且性能好，分析准确，能满足问题全部要求 | 非标讨论题：小组方案较合理，分析较正确，能基本满足问题全部要求 | 非标讨论题：小组方案基本合理，能满足问题大部分要求 | 非标讨论题：小组方案不够合理，只能满足问题少量要求 |
| | 标准讨论题：按照题目评分标准据实评价 | | | |
| 实验验收 | 按照每次实验的评分标准据实评价 | | | |

| | |
|---|---|
| 期末闭卷考试 | 按照期末试卷评分标准据实评价 |

## 八、 教学资源

**表 8 课程的基本教学资源**

| 资源类型 | 资源 |
|---|---|
| **教 材** | 陈伟、李频《网络安全原理与实践》，清华大学出版社，2014 |
| **参考书籍或文献** | （1）蔡红柳，何新华．信息安全技术及应用实验．北京：科学出版社，2004.10．<br>（2）Stallings，W. Cryptography and Network Security：Principles and Practice(Second Edition).清华大学出版社，2002.6.<br>（3）Stallings,W. 密码编码学与网络安全：原理与实践(第二版).电子工业出版社，2001.4.<br>（4）杨波.网络安全理论与应用.电子工业出版社，2002.1.<br>（5）赖溪松等.计算机密码学及其应用.国防工业出版社，2001.7<br>（6）郑鲲等，通信网络安全原理与实践，清华大学出版社，2014.7<br>（7）石志国等.计算机网络安全教程(第 2 版).清华大学出版社&北京交通大学出版社，2010 |
| **教学文档** | 无 |

## 九、 课程目标达成度定量评价

在课程结束后，需要对每一个课程目标（含思政课程目标）进行达成度的定量评价，用以实现课程的持续改进。

课程目标达成度的定量评价算法：

1、 使用教学活动（如课程思政实践、课后作业、课堂练习、实验验收、演讲、课堂讨论、互动、阅读报告等等）成绩或期末考试部分题目得分率作为评价项目，来对某个课程目标进行达成度的定量评价；

2、 为保证考核的全面性和可靠性，要求对每一个课程目标的评价项目选择超过两种；

3、 根据施教情况，评价项目可以由教师自行扩展，权重比例可以由教师自行设计；

4、 对某一个课程目标有支撑的各评价项目权重之和为 1；

5、 使用所有学生（含不及格）的平均成绩计算。

本课程的课程目标达成度的定量评价算法建议如表 10 所示，教师可根据授课方式及考核内容适当调整：

**表 9. 课程目标达成度定量评价方法**

| 课程目标 | 课程目标达成度评价方式 |
|---|---|
| **课程目标 1**：能够基于网络安全基本原理知识，了解发展趋势及其对社会发展的影响。能够运用网络安全基本原理和专业知识，分析处理网络系统运行过程中遇到的实际问题。 | 课后作业：0.1<br>在线测试：0.2<br>课堂参与/小组讨论：0.2<br>实验验收：0.2<br>期末考试：0.3 |
| **课程目标 2**：初步具备基本的网络安全功能原理、常用协议的分析能力。 | 课后作业：0.3<br>课堂参与/小组讨论：0.3<br>期末考试：0.4 |

| 课程目标 | 课程目标达成度评价方式 |
| --- | --- |
| **课程目标 3**：初步具备在真实网络条件下，设计组建计算机网络安全防护系统的能力；具备开发简单的计算机网络安全系统的能力。 | 课堂参与/小组讨论：0.2<br>课后作业：0.1<br>实验验收：0.3<br>期末考试：0.4 |
| **课程目标 4**：具有自主学习和终身学习意识及团队协作精神。 | 课堂参与/小组讨论：0.2<br>在线测试：0.2<br>实验验收：0.3<br>期末考试：0.3 |
| **课程目标 5**：具备客观辩证、探索创新等基本科学素养，及时了解网络安全的国内外新技术和发展趋势，了解国家在相关方面的网络安全战略需求，树立强烈的爱国主义使命感与责任心。 | 课程思政实践：0.5<br>课堂参与/小组讨论：0.2<br>期末考试：0.3 |

## 十、 说明

本课程大纲主要用于规范杭州电子科技大学计算机科学与技术、智能财务(软件工程)专业的《网络安全原理与实践》课程的教学目标、教学内容、教学方法、教学要求以及考核评价方法等，承担该课程的教师必须遵照本大纲安排授课计划、实施教学过程，完成学生各个阶段与各方面的学习成果考核与评价；在学期末，需对课程目标和课程支撑的毕业要求指标点进行达成度评价。

本课程大纲自 2021 级开始执行，生效之日原先版本均不再使用。

## 十一、编制与审核

**表 10. 大纲编制与审核信息**

| 工作内容 | 责任部门或机构 | 负责人 | 完成时间 |
| --- | --- | --- | --- |
| 编制 | 网络与信息安全课程组 | 张彦斌 | 2022.01.05 |
| 审核 | 网络与信息安全课程组 | 徐建 | 2022.01.10 |
| 审定 | 计算机学院教学工作委员会 | 袁友伟 | 2022.05.17 |