**北京市高等教育自学考试课程考试大纲**

**课程名称：信息安全基础 课程代码：14481（笔试） 2024年9月版**

**第一部分课程性质与设置目的**

**一、课程性质与特点**

《信息安全基础》是北京市高等教育自学考试计算机应用技术（专科）专业的一门专业课程，是在完成公共基础课程学习后开设的选考课。《信息安全基础》是计算机科学类专业的一门选修课程，它是一门新兴的研究软件开发与维护的普通原理和技术的工程学科。本课程的主要任务是掌握密码学是信息安全的基础组成部分，包括对称加密、非对称加密、哈希函数、数字签名等技术。这些技术可以用于保护数据的机密性、完整性以及身份验证。系统安全涉及操作系统、硬件和软件的安全防护。这包括对恶意软件（如病毒、木马、蠕虫等）的防护，以及保障系统免受未经授权的访问和敏感信息的泄露。网络安全关注网络基础设施的安全性，如互联网、内部网络和外部网络等。这包括防范网络攻击，如拒绝服务攻击（DoS）、分布式拒绝服务攻击（DDoS）、网络钓鱼等，保证网络通信的安全性和隐私性。应用安全涉及各种应用程序的安全性。这包括Web应用程序安全、数据库安全、电子邮件安全等，防止应用程序被恶意攻击和数据泄露。数据库安全主要关注保障数据库中数据的安全性和完整性。这包括对SQL注入、跨站脚本攻击（XSS）等攻击的防护，以及数据的备份和恢复等。信息安全法规与合规性是组织遵循国家和地方政策、法规以及行业标准，保障信息安全的重要部分。培养高层次软件开发设计人员，培养软件项目管理人员。

**二、课程目标与基本要求**

本课程的目标是全面贯彻落实立德树人根本任务，具体目标如下：对信息安全策略的制定和实施，以及合规性的审计和报告等。安全管理涉及到信息安全政策和制度的制定和实施，包括安全培训、安全意识提升、应急响应计划等。安全管理能够确保组织在面临信息安全事件时，能够及时响应并恢复。风险评估与应对是信息安全的重要环节，包括对组织面临的信息安全风险的评估和应对。这涉及到对潜在威胁的识别、漏洞的扫描和修复、安全审计等。通过风险评估与应对，组织可以有效地减少信息安全风险，提高信息安全的保障能力。安全架构与设计是信息安全的基础设施建设，包括信息安全的整体架构设计、安全技术的选型和应用、安全设备的配置和优化等。一个良好的安全架构和设计能够有效地提高组织的信息安全水平，减少信息安全事件的发生。通过团队建设和管理，培养学生团队合作，知识传递能力，独立完成团队分配的任务。总之，该课程需要同学们掌握软件项目管理的理论知识、技能和方法，以便更好地应对复杂多变的软件开发环境。具有团队合作精神和良好的沟通与表达能力，能够在多学科团队和跨文化环境下工作。在工程实践中遵守法律法规，遵循职业道德与工程标准，具有良好的社会责任感。能够快速适应环境，具有一定的专业技术洞察力和前瞻视野，具有终身学习的愿望、能力与技能，具有职业可持续发展的潜能，并能够胜任其他领域与软件工程相关的工作。

本课程的考核章节为第一章到第十章，重点章节是：第二章、第四章、第五章、第六章、第八章，一般考核章节为第一章、第三章、第七章、第九章、第十章，不考核章节无。

**三、与本专业其他课程的关系**

《信息安全基础》课程在的教学计划中被列为专业课，本课程与计算机基础与应用技术，计算机程序设计基础，数据库及应用等课程之间有承前启后的相互联系作用，本课程的学习对全面掌握软件技术专业各学科的知识起重要的桥梁作用。

**第二部分考核内容与考核目标**

**第一章 信息安全概述**

**一、学习目的与要求**

通过本章学习，要求学生了解信息安全的基本概念及网络信息安全的标准，对信息安全的重要性及研究内容有一个初步了解。

**二、考核知识点与考核目标**

识记：

1. 信息安全基本概念。
2. 信息安全面临的威胁。

理解：

1. 信息安全保障的技术体系和实施框架。
2. 常见的信息安全模型及其作用。

**第二章 信息安全基本保障技术**

**一、学习目的与要求**

通过本章的学习，要求学生了解随着信息技术的快速发展，信息安全已成为企业生存和发展的关键因素之一。信息安全不仅关系到企业的资产保护，还与企业的业务连续性、法规合规、形象提升、预防欺诈、保障隐私、知识产权保护以及防止网络攻击等方面有着密切的关联。信息安全是保护企业资产的重要组成部分。企业的资产包括但不限于金钱、固定资产、无形资产等。通过保障信息安全，可以避免企业资产在未经授权的情况下被访问、修改或破坏，从而确保资产的安全和完整性。

**二、考核知识点与考核目标**

识记：

1. 密码学的发展史，现代密码学。

2）数字签名的基本概念。

理解：

1. 对称与非对称密码学。
2. 图像隐藏技术和图像的数字化处理，音频和文本隐藏技术。
3. LSB图像信息隐藏实践的实践环境和实践步骤。

应用：

1. RSA算法。
2. ISES客户端对称密码基本加密实践。

**第三章 认识病毒及其防御技术**

**一、学习目的与要求**

通过本章的学习，要求学生掌握随着信息技术的不断发展，了解计算机病毒和特点。掌握典型的病毒的传播特点及危害。了解和掌握常见病毒的防御技术。掌握病毒防治工具的使用。

**二、考核知识点与考核目标**

识记：

1）病毒的定义和感染的策略，躲避侦测的方法。

2）病毒的主要特征，分类。

3）灰鸽子木马和特洛伊木马的特点。

理解：

1. 基于主机和基于网络的病毒防御技术。
2. 计算机网络病毒的防治方法。

应用：

1. 病毒的自启动技术。
2. 移动存储型病毒实践，病毒的简单结构和制作病毒文件。

**第四章 网络攻击与防御技术**

**一、学习目的与要求**

通过本章的学习，要求学生了解网络威胁的一般形式，了解网络攻击的一般方法，掌握常见的网络攻击方式的防御，掌握网络加固的一般方法。

**二、考核知识点与考核目标**

识记:

1）网络攻击的危害，黑客。

2）IP地址 和 ARP地址解析协议 ,DNS解析。

3）密码破解的常见形式。

4）搭建网络实现ARP地址欺骗过程。

理解：

1）网络攻击的一般方法和基本流程。

2）IP欺骗攻击流程和ARP欺骗原理，DNS欺骗 ，拒绝服务攻击和DDOS攻击。

3）APR地址欺骗攻击实践的原理，实践环境的配置。

应用：

1. 破解工具的使用，NTPWEdit，QQ密码破解，压缩文件破解，PDF文件密码破解。
2. APR地址欺骗攻击实践的步骤：包括设定环境，设置主机欺骗。

**第五章 网络设备安全技术**

**一、学习目的与要求**

通过本章的学习，要求学生了解防火墙，入侵检测，虚拟专用网，网络隔离和统一威胁管理系统的概念，掌握防火墙，入侵检测，虚拟专用网等关键技术，了解相关网络安全的常见产品。

**二、考核知识点与考核目标**

识记：

1. 防火墙的含义和功能，防火墙的局限性。
2. 网络地址转换NAT的含义。
3. 入侵检测系统的组成。
4. VPN的定义，分类。
5. 网络隔离技术的特点。

理解：

1. 防火墙包过滤技术，应用网关技术，代理服务器的原理。
2. NAT技术的原理，技术的类型，优缺点和局限性。
3. 入侵检测系统的功能，分类，局限性，入侵检测系统的发展方向。
4. VPN的关键技术，用户认证技术，解决方案。
5. 网络隔离技术的工作原理，技术类型。

应用：

站点到站点的IPSec VPN实现。

**第六章 无线网络安全技术**

**一、学习目的与要求**

通过本章的学习，要求学生了解无线传输协议，掌握WEP和 WPA加密方式，了解4G移动通信安全问题。

**二、考核知识点与考核目标**

识记：

1. 无线局域网的概念。
2. 802.11发展历史。
3. WEP的发展史。
4. 4G移动通信技术简介,5G时代的展望。

理解：

1. 无线局域网存在的安全隐患，安全威胁。
2. 安全技术体系--WEP包含的技术，标准，认证协议。
3. WEP的加密特点，安全隐患，WPA加密，WPA2加密。
4. 4G移动通信的无线网络安全防护措施。

应用：

利用BackTrack提供的工具破解目的AP的WEP密码。

**第七章 网络操作系统安全技术**

**一、学习目的与要求**

通过本章的学习，要求学生掌握网络安全技术是指应用在网络环境中，以保护计算机系统、网络设备和用户数据免受未经授权的访问、破坏和攻击的各种方法和策略。 这些技术包括防火墙、入侵检测系统、加密技术、访问控制机制等，旨在提供保护网络安全的基本层面。

**二、考核知识点与考核目标**

识记：

1. Kerberos V5详细的认证步骤。
2. 文件系统的概念。
3. 组策略概述。
4. linux发展史和系统架构。

理解：

1. Windows典型的操作系统 。
2. 单点登录身份认证执行方式，主要的身份认证类型。
3. Kerberos V5身份认证的优点与缺点。
4. NTFS文件系统，EFS文件加密，弹性文件系统。
5. 组策略概述基础架构，本地策略和域组策略。
6. linux的特点。

应用：

1. 用户和组安全--用户账号与口令管理。

**第八章 数据库安全技术**

**一、学习目的与要求**

通过本章的学习，要求学生了解和掌握数据库安全指的是对数据库进行保护，以确保其数据的机密性、完整性和可用性，并防止非法访问、篡改、破坏、泄露等安全威胁。了解数据的定义和应用，了解数据安全的重要性。

**二、考核知识点与考核目标**

识记：

1. 数据库的定义和分类。
2. 数据库的安全控制机制。

理解：

1. 数据库的特点。
2. SQL语言的分类和作用。
3. 云端数据库安全问题，云端数据库的优点，数据库的威胁与防护。

应用：

SQL Server的安全配置

1. 使用安全的密码策略。
2. 使用安全的账号策略。
3. 查看数据库日志。
4. 管理SQL Server内置存储过程XP\_cmdshell控制系统。

**第九章 信息系统安全测评与信息安全风险评估**

**一、学习目的与要求**

通过本章的学习，要求学生了解信息系统安全评测的概念，信息安全风险评估的目的和意义。知道信息安全测评与信息风险评估之间的关系。

1. **考核知识点与考核目标**

识记：

1）信息系统安全保护等级的定级要素。

2）信息安全风险评估的原则。

3）信息安全风险评估的概念。

理解：

1. 信息安全风险评估的分类。
2. 信息安全风险评估与等级保护的关系。

**第十章 信息安全法律法规**

**一、学习目的与要求**

通过本章的学习，要求学生了解信息安全相关法律法规概况。了解我国信息安全法律法规体系框架及其各个不同层面包括的基本内容。了解我国目前信息安全法律体系的主要特点。掌握信息安全从业人员的道德规范。

1. **考核知识点与考核目标**

识记：

1）构建信息安全法律法规的意义。

2）我国信息安全法律法规体系框架。

理解：

1）我国目前信息安全法律体系主要特点。

2）信息安全从业人员道德规范。

**第三部分有关说明与实施要求**

**一、考核的能力层次表述**

本大纲在考核目标中，按照“识记”、“理解”、“应用”三个能力层次规定其应达到的能力层次要求。各能力层次为递进等级关系，后者必须建立在前者的基础上，其含义是：

识记：能知道有关的名词、概念、知识的含义，并能正确认识和表述，是低层次的要求。

理解：在识记的基础上，能全面把握基本概念、基本原理、基本方法，能掌握有关概念、原理、方法的区别与联系，是较高层次的要求。

应用：在理解的基础上，能运用基本概念、基本原理、基本方法联系学过的多个知识点分析和解决有关的理论问题和实际问题，是最高层次的要求。

**二、指定教材**

《信息安全基础（第三版）》，徐振华 主编，高等教育出版社，2021年版。

**三、学习方法指导**

1、在开始阅读指定教材某一章之前，先翻阅大纲中有关这一章的考核知识点及对知识点的能力层次要求和考核目标，以便在阅读教材时做到心中有数，有的放矢。

2、阅读教材时，要逐段细读，逐句推敲，集中精力，吃透每一个知识点，对基本概念必须深刻理解，对基本理论必须彻底弄清，对基本方法必须牢固掌握。

3、在自学过程中，既要思考问题，也要做好阅读笔记，把教材中的基本概念、原理、方法等加以整理，这可从中加深对问题的认知、理解和记忆，以利于突出重点，并涵盖整个内容，可以不断提高自学能力。

4、完成书后作业和适当的辅导练习是理解、消化和巩固所学知识，培养分析问题、解决问题及提高能力的重要环节。在做练习之前，应认真阅读教材，按考核目标所要求的不同层次，掌握教材内容，在练习过程中对所学知识进行合理的回顾与发挥，注重理论联系实际和具体问题具体分析，解题时应注意培养逻辑性，针对问题围绕相关知识点进行层次（步骤）分明的论述或推导，明确各层次（步骤）间的逻辑关系。

**四、对社会助学的要求**

1、应熟知考试大纲对课程提出的总要求和各章的知识点。

2、应掌握各知识点要求达到的能力层次，并深刻理解对各知识点的考核目标。

3、辅导时，应以考试大纲为依据，指定的教材为基础，不要随意增删内容，以免与大纲脱节。

4、辅导时，应对学习方法进行指导，宜提倡"认真阅读教材，刻苦钻研教材，主动争取帮助，依靠自己学通"的方法。

5、辅导时，要注意突出重点，对考生提出的问题，不要有问即答，要积极启发引导。

6、注意对应考者能力的培养，特别是自学能力的培养，要引导考生逐步学会独立学习，在自学过程中善于提出问题，分析问题，做出判断，解决问题。

7、要使考生了解试题的难易与能力层次高低两者不完全是一回事，在各个能力层次中会存在着不同难度的试题。

8、助学学时：本课程共4学分，建议总课时72学时，其中助学课时分配如下：

|  |  |  |
| --- | --- | --- |
| 章 次 | 内 容 | 学 时 |
| 第一章 | 信息安全概述 | 4 |
| 第二章 | 信息安全基本保障技术 | 8 |
| 第三章 | 认识病毒及其防御技术 | 8 |
| 第四章 | 网络攻击与防御技术 | 10 |
| 第五章 | 网络设备安全技术 | 8 |
| 第六章 | 无线网络安全技术 | 8 |
| 第七章 | 网络操作系统安全技术 | 8 |
| 第八章 | 数据库安全技术 | 10 |
| 第九章 | 信息系统安全测评与信息安全风险评估 | 4 |
| 第十章 | 信息安全法律法规 | 4 |
| 合 计 | | 72 |

**五、关于命题考试的若干规定**

1．本大纲各章所提到的内容和考核目标都是考试内容。试题覆盖到章，适当突出重点。

2．笔试的比例一般为识记占40%，理解占40%，应用占20%。

3. 试题难易程度应合理：易、中等难度、难。难题部分比例不超过20%。

4．笔试试题类型一般分为：单项选择题、多项选择题、名词解释题、简答题、应用题。

5．笔试采用闭卷考核方式，考试时间 150分钟，按百分制计分，60分为及格。

**六、题型示例**

（一）单项选择题

包过滤防火墙工作在

1. 物理层 B. 数据链路层C. 网络层D. 应用层

（二）多项选择题

Kerberos V5身份认证的优点包括

A．支持相互身份认证 B.支持委派身份认证 C.简化的信任管理 D.采用非对称加密机制，密钥安全性高

（三）名词解释题

DNS欺骗

（四）简答题

云端数据库的优点

（五）应用题

某企业的总部和分部分别位于不同的城市，根据业务需要，现在要在总部和分部间建立可靠的信息传输。考虑到建设成本和原有设备的充分利用，该企业采用了VPN解决方案，并在原有的防火墙系统上配置VPN系统，实现站点到站点的可靠信息传输。

请描述基础配置环境、以总部防火墙的VPN为例的配置步骤。