高纲4389

江苏省高等教育自学考试大纲

04751　计算机网络安全

南京航空航天大学编（2025 年）

Ⅰ　课程性质与课程目标

一、课程性质和特点

《计算机网络安全》是江苏省高等教育自学考试网络工程专业（专升本）考试计划中的一门选设课。该课程是一门计算机领域的应用性和实践性较强的专业课程。主要涉及计算机网络安全基本理论和应用技能。本课程对于培养考生的逻辑思维、实践能力和创新能力都起到重要作用。通过本课程，考生可以获得计算机网络安全方面的基本理论知识和基本技能，了解计算机网络安全技术的应用现状和发展概况，为学习后继课程以及从事与本专业有关的计算机应用工作打下一定的基础。

二、课程目标

通过本课程的学习，考生应掌握计算机网络安全的基本概念，对计算机网络安全面临的威胁、应对的安全手段能有一个总体上的认知和把握。熟悉计算机网络安全涉及的各领域知识，在将来工作中对信息系统需要的安全措施、安全方案能够有系统性的认知和恰当的设置或者使用。

三、与相关课程的联系与区别

本课程的先修课程为《计算机网络原理》《C++程序设计》。

本课程在学习内容及学习环节等方面与相关课程的联系与分工如下：对于《计算机网络原理》课程，需要一些网络的基础知识、基本运行原理和基本的网络方面的程序设计知识；对于《C++程序设计》课程，需要具有相当的程序设计能力，可以自主设计/编写一定的小型应用系统。

四、课程的重点和难点

本课程包含主要内容有：网络安全概述、网络安全技术基础、网络安全体系与管理、黑客攻防与检测防御、密码与加密技术、身份认证与访问控制、计算机及手机病毒防范、防火墙技术及应用、操作系统及站点安全和数据库及数据库安全等。

重点和难点：网络安全涉及的相关理论及防御的相关技术和理论，如网络体系、协议、加密技术和身份认证技术等。

II　考核目标

本大纲在考核目标中，按照识记、领会、应用三个层次规定其应达到的能力层次要求。三个能力层次是递升的关系，后者必须建立在前者的基础上。各级能力层次的含义是：

识记：要求考生能够识别和记忆本课程中有关信息系统的相关概念、定义、方法、技术、应用、理论等，并能够根据考核的不同要求，做正确的表述、选择和判断。

领会：要求考生能够领悟和理解本课程中有关管理信息系统概念、理论方法的内涵及外延，理解信息系统中采用相关方法的理论支持及其符合条件及范围，能够鉴别关于概念和方法中不甚精准的说法；掌握相关知识的联系与差异，并能根据考核要求的不同层级对信息系统进行分析，做出正确的判断、解释和说明。

应用：考生能够运用本大纲规定的知识点，分析并解决相关的应用问题。具体到本课程中，考生能根据实际工作需要，将计算机网络安全方法运用到实践中。

III　课程内容与考核要求

第 1 章　网络安全概述

一、学习目的与要求

本章集中介绍网络安全的概念、网络安全技术和网络安全的威胁及发展态势。要求掌握网络安全和网络安全技术的基本概念。

二、考核知识点与考核要求

识记：①网络安全的相关概念、网络安全的目标和特征；②网络安全技术中的 PDRR 模型和 IPDRRR 模型；③网络安全面临主要威胁的种类。

三、本章的重点和难点

本章的重点和难点是：①网络安全和网络安全技术的基本概念。

第 2 章　网络安全技术基础

一、学习目的与要求

本章介绍了常用的网络安全技术基础知识、TCP/IP 层次安全及常用技术、IPv6、虚拟专用网（VPN）技术和无线网络安全技术。要求掌握 IPv6、虚拟专用网（VPN）技术和无线网络安全技术。

二、考核知识点与考核要求

识记：①网络安全技术的基础知识；②TCP/IP 层次安全及常用技术。

领会：①IPv6 的优势与特点、IPv6 相比 IPv4 在网络安全上的变化、IPv6 的安全机制和移动 IPv6 的特性；②虚拟专用网（VPN）的基本概念、技术特点、关键技术和实用解决方案；③无线网络接入点安全和 IEEE802.1x 认证过程。

应用：①IEEE802.1x 认证过程。

三、本章的重点和难点

本章的重点和难点是：①IPv6 的优势与特点、IPv6 相比 IPv4 在网络安全上的变化、IPv6 的安全机制和移动 IPv6 的特性；②虚拟专用网（VPN）的关键技术和实用解决方案；③无线网络接入点安全和 IEEE802.1x 认证过程。

第 3 章　网络安全体系与管理

一、学习目的与要求

本章集中介绍网络安全管理与保障体系和网络安全管理的基本过程、概述了国外在网络安全方面的法律法规和我国网络安全方面的法律法规。要求掌握网络安全体系和网络安全管理。

二、考核知识点与考核要求

识记：①ISO 网络安全体系结构和 TCP/IP 网络安全体系结构；②网络安全相关法律法规；③网络安全评估准则和方法。

领会：①ISO 网络安全体系结构中网络安全机制和网络安全服务；②TCP/IP 网络安全管理体系结构；③网络安全保障体系。

三、本章的重点和难点

本章的重点和难点是：①ISO 网络安全体系结构中网络安全机制和网络安全服务；②TCP/IP 网络安全管理体系结构。

第 4 章　黑客攻防与检测防御

一、学习目的与要求

本章集中介绍黑客攻击的步骤、黑客攻防技术、入侵检测和防御系统。要求掌握黑客攻击技术和检测防御技术。

二、考核知识点与考核要求

识记：①黑客的相关概念、黑客攻击的目的和过程；②网络攻击的防范措施。

领会：①端口扫描的攻防、网络监听的攻防、社会工程学的攻防、密码破解的攻防、缓冲区溢出的攻防、拒绝服务的攻防、特洛伊木马的攻防和网络欺骗的攻防；②入侵检测和防御系统的基本原理。

应用：①入侵检测系统原理及功能。

三、本章的重点和难点

本章的重点和难点是：①黑客攻防技术；②入侵检测和防御系统。

第 5 章　密码与加密技术

一、学习目的与要求

本章集中介绍密码技术相关概念、密码破译方法与密钥管理、实用加密技术。要求掌握密码与加密相关技术。

二、考核知识点与考核要求

识记：①密码学基本概念和基本术语；②密码体制及其分类；③数据及网络加密方式；④密码破译方法与密钥管理；⑤信息隐藏技术和量子密码。

领会：①密码系统基本原理；②非对称密码体制；③单向加密体制；④WEP 加密技术。

应用：①古典密码体制中置换密码；②对称密码体制。

三、本章的重点和难点

本章的重点和难点是：①实用加密技术。

第 6 章　身份认证与访问控制

一、学习目的与要求

本章集中介绍身份认证技术、数字签名技术、访问控制技术和网络安全审计。要求掌握身份认证和访问控制相关技术。

二、考核知识点与考核要求

识记：①身份认证的基本概念；②访问控制的基本概念；③网络安全审计。

领会：①身份认证的常用方式；②访问控制实现方法、访问控制模型和认证服务与访问控制系统；③数字签名方法和功能。

应用：①数字签名的签名和验证过程。

三、本章的重点和难点

本章的重点和难点是：①数字签名技术的原理。

第 7 章　计算机及手机病毒防范

一、学习目的与要求

本章集中介绍病毒的概念、特点、种类、危害、构成和传播，病毒的检测、清除和防范。要求掌握病毒相关概念及防范措施。

二、考核知识点与考核要求

识记：①病毒的基本概念和发展阶段；②病毒的特点和种类；②病毒的检测、清除和防范。

领会：①病毒的构成、传播、触发和生存；②木马病毒和蠕虫病毒。

三、本章的重点和难点

本章的重点和难点是：①病毒的构成、传播、触发和生存；②木马病毒和蠕虫病毒。

第 8 章　防火墙技术及应用

一、学习目的与要求

本章集中介绍防火墙基本概念、防火墙技术类型、防火墙的应用。要求掌握防火墙基本原理。

二、考核知识点与考核要求

识记：①防火墙基本概念、特点、主要缺陷和常用类型。

领会：①包过滤型防火墙和应用代理型防火墙；②防火墙阻止 SYN Flood 攻击。

应用：①防火墙的主要应用。

三、本章的重点和难点

本章的重点和难点是：①包过滤型防火墙和应用代理型防火墙；②防火墙阻止 SYN Flood 攻击；③防火墙的主要应用。

第 9 章　操作系统及站点安全

一、学习目的与要求

本章集中介绍 Windows 操作系统、UNIX 操作系统、Linux 系统的安全和 Web 站点的安全。要求掌握操作系统及站点安全。

二、考核知识点与考核要求

识记：①Linux 操作系统安全；②UNIX 操作系统安全。

领会：①Windows 操作系统安全；②Web 站点的安全。

三、本章的重点和难点

本章的重点和难点是：①Windows 操作系统安全；②Web 站点的安全。

第 10 章　数据库及数据库安全

一、学习目的与要求

本章集中介绍数据库安全体系与防护、数据库安全措施、数据库安全策略和机制。要求掌握数据库安全策略和机制。

二、考核知识点与考核要求

识记：①数据库及数据安全相关概念和数据库系统面临的安全问题；②可信 DBMS 体系结构；③数据库的安全防护；④数据库备份和恢复。

领会：①数据库安全的层次体系结构；②数据库的安全性、数据库及数据的完整性；③数据库的并发控制；④SQL Server 的安全机制。

三、本章的重点和难点

本章的重点和难点是：①数据库安全的层次体系结构；②数据库的安全性、数据库及数据的完整性；③数据库的并发控制。

第 11 章　电子商务安全（本章内容不作考核要求）

第 12 章　网络安全新技术及解决方案（本章内容不作考核要求）

第 13 章　网络安全课程设计指导（本章内容不作考核要求）

Ⅳ　关于大纲的说明与考核实施要求

一、自学考试大纲的目的和作用

自学考试大纲是根据专业考试计划的要求，结合自学考试的特点而确定。其目的是对个人自学、社会助学和课程考试命题进行指导和规定。

本课程自学考试大纲明确了本课程学习的内容以及深广度，规定了本课程自学考试的范围和标准。同时，大纲附有题型，使考试标准具体化。自学考试的大纲是自学考试命题的依据，也是对课程进行自学及助学的依据。

二、课程自学考试大纲与教材的关系

教材是学习掌握课程知识的基本内容与范围，课程自学考试大纲是进行学习和考核的依据，教材的内容是大纲所规定的课程知识和内容的扩展与发挥。

本大纲与教材所体现的课程内容完全一致；大纲里面的课程内容和考核知识点，教材里都能找到。

三、关于自学教材

本课程使用教材为：《网络安全技术及应用实践教程》（第 4 版），贾铁军、何道敬主编，机械工业出版社，2022 年。

四、关于自学要求和自学方法的指导

本大纲的课程基本要求是依据专业考试计划和专业培养目标而确定的。课程基本要求还明确了课程的基本内容，以及对基本内容掌握的程度。基本要求中的知识点构成了课程内容的主体部分。因此，课程基本内容掌握程度、课程考核知识点是高等教育自学考试考核的主要内容。

为有效地指导个人自学和社会助学，本大纲已指明了课程的重点和难点，在章节的基本要求中一般也指明了章节内容的重点和难点。

五、应考指导

1. 如何学习。本课程作为网络工程专业的一门重要课程，培养考生具有计算机网络安全方面的基本理论知识和基本技能。建议学习本课程时注意以下几点：

（1）在学习本课程教材之前应先仔细阅读本大纲，了解本课程的性质和特点，熟知本课程的基本要求，在学习本课程时，能紧紧围绕本课程的基本要求。

（2）在自学教材的每一章之前，先阅读本大纲中对应章节的学习目的与要求、考核知识点与考核要求，以使自学时做到心中有数。

（3）学习本课程的目的是掌握计算机网络安全的基本概念，对计算机网络安全面临的威胁，应对的安全手段有一个总体上的认知和把握。除要学习课程书本知识之外，应该多动手实践，从而熟练掌握网络病毒的预防、检测和清除等技术、方法和原理

2. 如何考试。卷面整洁非常重要。书写工整，段落与间距合理，卷面赏心悦目有助于教师评分，教师只能为他能看懂的内容打分。解答问题时，要审清题目，回答所提出的问题，避免超过问题的范围或者答非所问。

3. 如何处理紧张情绪。正确处理对失败的惧怕，要正面思考。如果可能，请教已经通过该科目考试的人，问他们一些问题。做深呼吸放松，这有助于使头脑清醒，缓解紧张情绪。考试前合理膳食，保持旺盛精力，保持冷静。

六、对社会助学的要求

1. 社会助学者应根据本大纲规定的考试内容和考核目标，认真钻研指定教材，明确本课程的特点和学习要求，对考生进行切实有效的辅导，避免考生在自学时可能出现的各种偏向，把握社会助学的正确方向。

2. 社会助学者应对考生进行学习方法的指导，向考生提倡“认真阅读教材，刻苦钻研教材，主动提出问题，依靠自己学懂”的学习方法。

3. 社会助学者应注意对考生自学能力的培养，使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、做出判断和解决问题。对考生提出的问题，社会助学者应以启发引导为主。

4. 社会助学者应指导考生正确处理重点和一般的关系。课程内容有重点与一般之分，但考试内容是全面的，而且重点与一般是相互影响的，不是截然分开的。社会助 学者应指导考生全面系统地学习教材，掌握全部考试内容和考核知识点，在此基础上再突出重点。总之，要把重点学习同兼顾一般结合起来，切勿孤立地抓重点，把考生引向猜题押题。

七、对考核内容的说明

本课程要求考生学习和掌握的知识点内容都作为考核的内容。课程中各章的内容均由若干知识点组成，在自学考试中成为考核知识点。大纲中按照不同知识点的重要程度分别确定其考核要求。

八、关于考试命题的若干规定

1. 考试方式为闭卷、笔试，考试时间为 150 分钟。评分采用百分制，60 分为及格。考生只准携带 0.5 毫米黑色墨水的签字笔、铅笔、圆规、直尺、三角板、橡皮等必需的文具用品，可携带没有存贮功能的普通计算器。

2. 本大纲各章所规定的基本要求、知识点及知识点下的知识细目，都属于考核的内容。考试命题既要覆盖到章，又要避免面面俱到。要注意突出课程的重点、章节重点，加大重点内容的覆盖度。

3. 命题不应有超出大纲中考核知识点的范围的题目，考核目标不得高于大纲中所规定的相应的最高能力层次要求。命题应着重考核考生对基本概念、基本知识和基本理论是否了解或掌握，对基本方法是否会用或熟练。不应出与基本要求不符的偏题或怪题。

4. 本课程在试卷中对不同能力层次要求的分数比例大致为：识记占 30%，领会占 40% ，应用占 30%。

5. 要合理安排试题的难易程度，试题的难度可分为：易、较易、较难和难四个等级。每份试卷中不同难度试题的分数比例一般为 2:3:3:2。必须注意试题的难易程度与能力层次有一定的联系，但二者不是等同的概念。在各个能力层次中对于不同的考生都存在着不同的难度，切勿混淆。

6. 本课程考试试卷中可能采用的题型有：单项选择题、判断改错题、简答题、论述题。

附录　题型示例

一、单项选择题

1．数据未经授权不能进行改变的特性是(　　)

A．保密性　　B．完整性

C．可用性　　D．可控性

参考答案：B

二、判断改错题

1．防火墙技术只能通过硬件设备实现，无法通过软件配置完成。（　　）

参考答案：×。“只能通过硬件实现，无法通过软件配置”改为“既能通过硬件实现，也能通过软件配置”。

三、简答题

1．简述“社会工程学攻击”的常见形式及防御措施。

参考答案：

常见形式：钓鱼邮件、假冒身份电话、伪装成合法机构的网站、尾随进入限制区域等。

防御措施：加强员工安全意识培训；验证请求者身份（如多因素认证）；制定严格的数据访问权限管理制度；部署反钓鱼技术（如邮件过滤、网站证书检测）。

四、论述题

1．论述当前物联网（IoT）面临的主要安全威胁及应对策略。

参考答案：

主要威胁：

（1）设备漏洞：硬件或固件缺陷导致未授权访问；

（2）数据泄露：传输或存储中数据未加密；

（3）僵尸网络攻击：设备被控制发起 DDoS 攻击；

（4）身份伪造：弱认证机制引发的伪装风险。

应对策略：

（1）技术层面：强制设备端到端加密；定期更新固件修补漏洞；部署轻量级认证协议（如 DTLS）。

（2）管理层面：制定物联网安全标准与法规；厂商需遵循“安全设计”原则（Security by Design）；用户侧加强密码管理与网络分段隔离。