湖南省高等教育自学考试

课 程 考 试 大 纲

信息安全导论

（课程代码：01583）

湖南省教育考试院组编
2021 年 6 月

高等教育自学考试课程考试大纲

课程名称：信息安全导论　　课程代码：　01583

第一部分 课程性质与目标

一、课程性质与特点

信息安全导论是高等教育自学考试软件技术（专科）专业的选考课程，通过本课程的学习，使考生对信息安全领域的知识与技能有深入了解，能掌握信息安全各个方面的安全管理技术。

本课程系统地介绍了信息安全的基础知识、安全技术及其应用。内容包括网络操作系统安全、网络实体安全、网络数据库与数据安全、数据加密技术与应用、网络攻防技术、互联网安全、无线网络安全和典型的网络安全应用实例。考生在学习后能够了解和掌握一定的网络安全知识、技术和实用技能，能针对不同的安全需求采取正确的措施保护网络环境的安全可靠。

二、课程目标与基本要求

（一）课程目标：通过本课程的学习，考生能对信息安全技术从整体上有一个较清晰的、全面的、系统的了解，对当前信息安全领域面临的各种威胁能够进行有效分析，理解攻击实施的方法与原理，能够提出防御或者解决方案，通过实施与部署，从根源上缓解或者清除安全威胁。

（二）基本要求：

1. 了解网络安全的体系结构与评价准则；
2. 了解常见操作系统面临的安全威胁与防御方法；
3. 掌握数据库面临的安全威胁与防御方法；
4. 掌握常见密码学体系结构与经典加解密方法；
5. 掌握木马、防火墙等网络攻防技术；
6. 掌握互联网应用安全技术；
7. 掌握无线网络安全防护机制。

三、与本专业其他课程的关系

本课程在软件技术（专科）专业的教学计划中被列为专业基础课程，是众多专业课程的先修课程，与本专业的其它网络类课程有着密切的关系，例如后继课程《网络应用程序设计》。本课程无先修课程。

第二部分 考核内容与考核目标

第 1 章 网络安全概述

一、学习目的与要求

通过本章学习，了解网络安全的概念、特征和安全目标，理解网络安全的威胁和风险，理解网络安全体系结构，网络安全的策略和技术，了解网络安全的评价准则和网络系统安全的日常管理。

二、考核知识点与考核目标

（一）网络安全概论（一般）

识记：网络安全的概念

理解：网络安全目标（可用性、可靠性、机密性、完整性、不可抵赖性、可控性）

（二）网络安全面临的威胁与风险（一般）

识记：网络安全的风险评估

理解：网络安全漏洞的类型（网络协议漏洞、网络服务漏洞等）

网络安全的威胁（物理威胁、操作系统缺陷、网络协议缺陷、体系结构缺陷、黑客程序、计算机病毒）

（三）网络安全体系结构（重点）

识记：7 层 OSI 参考模型

5 种安全服务

8 种安全机制

理解：OSI 安全体系

P2DR 网络安全模型

P2RR 网络安全模型

（四）网络安全策略与技术（次重点）

理解：网络安全策略（物理安全策略、访问控制策略、信息加密策略、安全管理策略）

网络安全技术（安全漏洞扫描技术、网络嗅探技术、数据加密技术、数字签名技术、鉴别技术、访问控制技术、安全审计技术、防火墙技术、入侵检测、病毒防范技术）

（五）网络安全评价准则（一般）

识记：可信计算机系统评价准则

计算机信息安全保护等级划分准则

（六）网络系统的安全管理（一般）

识记：网络系统安全维护的几个方面：口令管理、病毒防护、漏洞扫描、边界控制、实时监控、日志审核、应急响应、软件和数据文件保护

理解：网络系统的日常管理

网络日志管理

第 2 章 网络操作系统安全

一、学习目的与要求

通过本章学习，掌握计算机网络操作系统提供的安全管理措施与访问控制方法，了解不同操作系统的特点与安全工具，各类操作系统存在的系统漏洞及其防御方法。

二、考核知识点与考核目标

（一）网络操作系统简介（一般）

识记：Windows Server 2008 系统及其特点

UNIX 系统及其特点

Linux 系统及其特点

Android 系统及其特点

iPhone 操作系统及其特点

（二）网络操作系统的安全与管理（重点）

识记：网络操作系统安全保护的研究内容

访问控制系统的组成

访问控制的类型

常用的身份认证方法

理解：Windows Server 2008 系统安全

UNIX 系统安全

Linux 系统安全（身份验证机制、用户权限体系、文件加密机制、安全系统日志和审计机制、强制访问控制）

Linux 安全工具的使用

Android 系统安全

iPhone 操作系统安全

第 3 章 网络实体安全

一、学习目的与要求

通过本章学习，掌握硬件系统的冗余、网络机房设施与环境安全、路由器安全、交换机安全、服务器安全和客户机安全的维护与管理。

二、考核知识点与考核目标

（一）网络硬件系统的冗余（次重点）

识记：冗余的含义

冗余的分类

RAID 的等级

理解：双机热备的概念

电源冗余和网卡冗余的应用场景

核心交换机冗余与链路冗余的关系

（二）网络机房设施与环境安全（次重点）

识记：机房及内部管理措施

机房环境监控系统监控的数据类型

机房的温度、湿度和洁净度的标准

UPS 的组成与功能

机房内引起火灾的原因与防范措施

机房内静电对网络设备的影响

机房内电磁防护的措施

（三）路由器安全（重点）

识记：路由器的工作原理

常见的路由算法

访问控制列表的作用与分类

理解：路由器口令的保密性

VRRP 功能与工作机制

VRRP 中的优先级概念

应用： 路由器常见的接入配置方法及安全性

路由器访问控制的安全策略

（四）交换机安全（重点）

识记：交换机的工作原理

交换机中 MAC 地址表的变化

理解：DDoS 攻击的防范

VLAN 的隔离功能

应用：802.1x 的认证机制

交换机中 ACL 的作用

交换机中端口安全的配置

交换机端口汇聚与镜像的配置

（五）服务器与客户机安全（一般）

识记：网络服务器的作用

网络服务器的分类

理解：服务器的安全策略

客户机的安全策略与风险防护

第 4 章 网络数据库与数据安全

一、学习目的与要求

通过本章学习，掌握网络数据库可能面临的安全威胁，熟悉网络数据库的安全特性和策略，掌握数据备份、恢复和容灾处理等措施。

二、考核知识点与考核目标

（一）网络数据库安全概述（一般）

识记：数据库安全的概念

数据库安全管理原则

理解：常见的数据库系统的安全漏洞与缺陷

数据库安全威胁的来源

（二）网络数据库的安全特性和策略（次重点）

识记：多用户数据库系统提供的安全机制

角色管理的优点

数据库角色的功能

理解：网络数据库的安全策略

数据库审计的方式

（三）网络数据库用户管理（重点）

理解：配置身份验证

应用：数据库用户管理

数据库权限管理

（四）数据备份、恢复和容灾（次重点）

识记：数据备份的概念

数据备份的目的

数据备份的类型

数据备份的策略

数据恢复的概念

数据恢复的注意事项

数据恢复的类型

理解： 数据容灾与数据备份的关系

容灾系统的核心技术与实施方案

SAN 与 NAS 的关系

（五）大数据及其安全（一般）

识记：大数据的概念

理解：大数据中的不安全因素

大数据的安全策略

第 5 章 数据加密技术与应用

一、学习目的与要求

通过本章学习，掌握密码学的数据加密体制，传统密码技术与现代密码技术的应用场景，了解数字签名的原理，掌握数字证书的原理与应用方法，掌握网络保密通信及其协议。

二、考核知识点与考核目标

（一）密码学基础（一般）

识记：密码学的基本概念

密码的分类

理解：传统密码技术（替代密码、移位密码、一次一密钥密码）

明文、密文、加密算法和密钥的关系

应用：替代密码

移位密码

（二）数据加密体制（次重点）

理解：对称密钥密码体制

公开密钥密码体制

DES 算法的原理

使用公开密钥对文件进行加密传输的步骤

RSA 算法

（三）数字签名与认证（重点）

识记：公钥基础设施 PKI

理解：数字签名的概念、功能、过程、算法

CA 认证与数字证书

数字证书的功能和应用

（四）网络保密通信（重点）

识记：常见的网络服务漏洞

SSL 协议的功能与工作层次

理解：不同层次上的加密

网络加密方式（链路加密、端到端加密）

应用：SSL 协议及应用

SSH 协议及应用

SET 协议及应用

Kerberos 协议及应用

IPSec 协议及应用

第 6 章 网络攻防技术

一、学习目的与要求

通过本章学习，掌握黑客攻击网络的常用手段，从而能够针对各种威胁部署安全防护设备和措施，清除入侵的危害并进行恢复处理。

二、考核知识点与考核目标

（一）防火墙安全（一般）

识记：防火墙的概念、主要功能、特征、不足之处

理解：常用的防火墙技术

（二）网络病毒与防范（次重点）

理解：计算机病毒的含义、特征、类型、传播途径、危害以及发展趋势

网络病毒的含义、特点、传播媒介

网络病毒类型与防范措施

（三）木马攻击与防范（重点）

理解：木马的概念、原理、危害

木马的预防措施和清除措施

（四）网络攻击与防范（重点）

理解：网络攻击的定义

黑客的定义，黑客攻击的主要类型、攻击的手段和工具

网络攻击的实施过程

应用：网络攻击的防范实例

（五）网络扫描、监听和检测（重点）

理解：网络扫描的含义、作用与分类

网络监听的含义与作用

网络入侵检测系统与技术

（六）虚拟专用网（重点）

理解：VPN 技术基础、VPN 的功能与特点

VPN 关键技术

网络中 VPN 的连接

第 7 章 互联网安全

一、学习目的与要求

通过本章学习，了解黑客盗取用户密码、网络病毒入侵、电子邮件攻击、网络交易欺骗等常见攻击手段的原理，从而能够针对这些威胁进行及时响应、处理与预防。

二、考核知识点与考核目标

（一）TCP/IP 协议及其安全（一般）

识记：TCP/IP 协议的层次结构和主要协议的功能

TCP/IP 协议的层次安全

理解：TCP/IP 协议的安全性分析

（二）Internet 欺骗（次重点）

理解：IP 电子欺骗含义、原理、过程与防范措施

ARP 电子欺骗的防范措施

DNS 电子欺骗的安全威胁、原理与防范措施

（三）网站安全（重点）

理解：Web 概述

Web 应用的安全威胁，Web 服务器、浏览器与传输的安全要求

Web 电子欺骗原理与防范措施

（四）电子邮件安全（重点）

理解：电子邮件的安全漏洞和威胁

电子邮件欺骗

电子邮件的安全策略

（五）电子商务安全（一般）

识记：电子商务概述

理解：电子商务的安全威胁

电子商务的安全对策

第 8 章 无线网络安全

一、学习目的与要求

通过本章学习，了解无线网络中窃听、假冒等攻击手段对用户造成的影响，掌握无线网络的安全机制从而保证信息的保密性、完整性和可用性。

二、考核知识点与考核目标

（一）无线网络的协议与技术（一般）

识记：无线广域网及技术标准

无线局域网及技术标准

（二）无线网络安全（次重点）

识记：蜂窝网络的概念

GSM 的认证过程

理解：无线网络存在的不安全因素与面临的主要威胁

常见的无线蜂窝网络类型及各类型的安全性

无线设备与数据安全

无线网络的安全机制

无线网络的安全措施

第 9 章 网络安全实践

一、学习目的与要求

通过本章学习，了解操作系统、网络设备、加密系统的安全管理方法，掌握对已知网络威胁进行预防，分析，恢复的策略与方法，具备处理网络攻击的能力。

二、考核知识点与考核目标

（一）常用网络工具的使用（次重点）

应用：常用网络工具 ping 和 ARP 的使用

（二）网络操作系统的安全设置（重点）

应用：Windows 7 系统的安全设置

Windows Server 2008 系统的安全设置

Linux 系统的安全设置

（三）网络部件的安全设置（重点）

应用：路由器安全设置

交换机安全设置

服务器安全管理

客户机安全管理

（四）数据加密技术的应用（重点）

应用：加密软件 PGP 及应用

RSA 密钥软件的应用

EFS 及应用

（五）网络安全防护的应用（重点）

应用：高级安全 Windows 防火墙设置

瑞星杀毒软件 V17 的应用

木马清除大师软件的应用

网络扫描工具应用实例

网络嗅探工具应用实例

缓冲区溢出攻击实例

VPN 配置实例

（六）互联网应用案例（重点）

应用：电子邮件的安全应用实例

网上购物安全交易过程

（七）无线网络路由器的安全设置（重点）

应用：无线网络路由器的安全设置

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、教材

指定教材：计算机网络安全（第 3 版），刘远生，清华大学出版社，2018 年

三、自学方法指导

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．注意对考生能力的培养，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 1 章	网络安全概述	4
第 2 章	网络操作系统安全	8
第 3 章	网络实体安全	8
第 4 章	网络数据库与数据安全	8
第 5 章	数据加密技术与应用	8
第 6 章	网络攻防技术	8
第 7 章	互联网安全	8
第 8 章	无线网络安全	8
第 9 章	网络安全实践	12
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.试卷中对不同能力层次的试题比例大致是：“识记”为 30%、“理解”为 40%、

“应用”为 30%。

3．试题难易程度应合理：易、中等、难比例为 3：4：3。

4．每份试卷中，各类考核点所占比例约为：重点占 60%，次重点占 30%，一般占 10%。

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

6．考试采用闭卷笔试，考试时间 150 分钟，采用百分制评分，60 分合格。

六、题型示例（样题）

一、单项选择题（本大题共■小题，每小题■分，共■分）

在每小题列出的四个备选项中只有一个是符合题目要求的，请将其选出并将“答题卡”上的相应字母涂黑。错涂、多涂或未涂均无分。

1. SSL 协议提供在客户端和服务器之间的

A．远程登录　　B．安全通信　　C．密钥安全认证　　D．非安全连接

二、多项选择题（本大题共■小题，每小题■分，共■分）

在每小题列出的五个备选项中至少有两个是符合题目要求的，请将其选出并将“答题卡”上的相应字母涂黑。错涂、多涂、少涂或未涂均无分。

2. 拒绝服务攻击的后果有

A．被攻击服务器资源耗尽　B．无法提供正常网络服务　C．被攻击者系统崩溃

D．被攻击者感染病毒　　E．被攻击者感染木马

三、填空题（本大题共■小题，每小题■分，共■分）

3．数据恢复操作的种类有_____、_____和重定向恢复。

四、名词解释题（本大题共■小题，每小题■分，共■分）

4．数字签名

五、简答题（本大题共■小题，每小题■分，共■分）

5．简述木马的预防措施。

六、应用题（本大题共■小题，每小题■分，共■分）

6. 网络中某台计算机抓取数据包的截图如下，请分析此计算机正在遭受什么样的攻击？可能带来哪些危害？怎样预防？