湖南省高等教育自学考试

课 程 考 试 大 纲

信息与网络安全管理

（课程代码：**03344**）

湖南省教育考试院组编

2016 年 **12** 月

高等教育自学考试课程考试大纲

课程名称：信息与网络安全管理　　课程代码：03344

第一部分　课程性质与目标

一、课程性质与特点

信息与网络安全管理是高等教育自学考试电子政务（本科）专业的专业核心课程、是电子商务（移动商务管理方向）（本科）专业的选考课程，其任务是培养电子政务与电子商务专业人才掌握信息与网络安全技术的理论知识和实际技能。

《网络安全与管理》为本课程指定教材，共分为 12 章，主要内容包括：网络安全概述、网络操作命令及协议分析、密码学基础、密码学应用、操作系统的安全机制、Web 安全、电子邮件安全、防火墙技术、计算机病毒与反病毒技术、网络攻防和入侵检测、网络管理原理、网络管理系统等方面的内容。本书概念准确、选材适当、结构清晰，注重理论与实践相结合，内容丰富、科学合理。

二、课程目标与基本要求

（一）课程目标：通过《网络安全与管理》课程的学习，使考生能够比较全面、系统地掌握网络与信息安全的理论和实践知识，帮助考生了解网络所面临的各种安全威胁、掌握网络安全的基本原理、掌握保障网络安全的主要技术和方法。学会在开放的网络环境中保护信息和数据，防止黑客和病毒的侵害，有效管理和使用计算机网络。

（二）基本要求：

1．需掌握相关的计算机知识，如计算机基础理论、操作系统、网络技术、密码学等。

2．理论与实践相结合，即将所学的相关信息安全知识与实际的电子政务系统信息安全相结合。

3．由于密码学中的加密算法是基于复杂的数学理论，对于电子政务专业的考生只要求大概理解，不作深入学习。

三、与本专业其他课程的关系

学习本课程应具备计算机程序设计和计算机网络等学科的知识基础条件。本课程的先修课程为：计算机基础与程序设计、计算机网络基础等。

第二部分　考核内容与考核目标

第一章　网络安全概述

一、学习目的与要求

本章介绍网络安全的基本概念和术语，分析网络安全现状、影响网络安全的因素；并阐述网络安全对于政治、经济、军事等方面的重要作用；最后分析国内外对信息安全的重视和立法情况，通过本章学习要求考生理解网络安全的基本概念和术语、了解目前主要的网络安全问题和安全威胁、理解基本的网络安全模型和功能、了解网络和信息安全的重要性、了解国内外信息安全保障体系。

二、考核知识点与考核目标

（一）网络安全的基本概念（重点）

识记：1．网络安全定义及相关术语；2．主要的网络安全威胁

理解：1．网络安全模型；2．网络安全策略

（二）网络体系结构及各层的安全性（重点）

识记：1．网络结构；2．TCP/IP 参考模型

理解：OSI-RM 及所提供的安全服务

（三）网络安全现状（次重点）

识记：网络安全现状

理解：研究网络安全的意义

（四）网络安全保障体系及相关立法（一般）

识记：1．美国政府信息系统的安全防护体系；2．中国网络安全保障体系

第二章 网络操作命令及协议分析

一、学习目的与要求

通过本章学习，要求考生了解常用的网络协议和服务、掌握协议分析工具和使用方法、掌握网络操作命令的使用。

二、考核知识点与考核目标

（一）常用网络协议和服务（次重点）

识记：常用网络协议

理解：常用网络服务

（二）协议分析工具－Sniffer 的应用（重点）

识记：Sniffer Pro 的启动和设置

理解：解码分析

应用：Sniffer

（三）Windows 常用的网络命令（重点）

识记：ping 命令、ipconfig 命令、tracert 命令、net 指令、nbtstat、ftp、telnet、netstat

理解：ipconfig 命令、tracert 命令、net 指令、nbtstat、ftp、telnet

应用：netstat 命令

第三章　密码学基础

一、学习目的与要求

本章主要讲述古典密码学和现代密码学的主要算法，通过本章学习，考生应该掌握以下内容：密码学的基本概念和术语、对称和非对称密码的区别、古典密码学的基本方法、掌握 DES 算法、RSA 算法的基本原理。

二、考核知识点与考核目标

（一）密码学概述（一般）

识记：1．密码系统；2．密码的分类

（二）古典密码学（次重点）

识记：1．代换密码；2．置换密码

（三）对称密码学（重点）

识记：1．分组密码概述；2．DES 算法；3．对称密码的工作模式

理解：1．分组密码的基本设计思想—Feistel 网络；2．其他的对称加密算法

（四）非对称密码体制（重点）

识记：1．RSA；2．Diffie-Hellman 算法

第四章　密码学应用

一、学习目的与要求

本章主要学习密码学应用方面的知识，包括密钥管理、消息认证、数字证书等，通过本章学习，要求考生掌握密钥的生命周期及密钥管理概念、对称密钥体制、公钥体制的密钥管理方法、消息认证的原理和方法、PKI 的原理、数字证书的应用以及 Windows2000 的证书服务。

二、考核知识点与考核目标

（一）密钥管理（重点）

识记：1．密钥产生及管理概述；2．对称密码体制的密钥管理

理解：公开密钥体制的密钥管理

（二）消息认证（重点）

识记：1．数据完整性验证；2．数字签名

理解：1．单向散列函数；2．消息摘要算法 MD5

（三）Kerberos 认证交换协议（重点）

识记：Kerberos 模型的工作原理和步骤

理解：Kerberos 的优势与缺陷

（四）公钥基础设施----PKI（重点）

识记：1．PKI 的定义、组成及功能；2．CA 的功能

理解：PKI 的体系结构

（五）数字证书（次重点）

识记：1．数字证书的类型及格式；2．证书的验证

理解：1．数字证书的管理；2．Windows 2000 Server 的证书服务

第五章　操作系统的安全机制

一、学习目的与要求

本章主要介绍常用的操作系统 Windows 2000 的安全机制和安全配置，通过本章学习，要求考生了解 Windows 2000 Server 的加密机制、了解 Windows 2000 Server 的认证机制、了解 Windows 2000 Server 的审计机制、熟练掌握 Windows 2000 Server 的基本安全配置。

二、考核知识点与考核目标

（一）Windows 2000 的认证机制（次重点）

识记：1．身份认证；2．消息验证；3．数字签名

（二）Windows 2000 的审计机制（一般）

识记：1．审核策略；2．审核对象的设置；3．选择审核项的应用位置

（三）Windows 2000 的加密机制（一般）

识记：1．文件加密；2．网络资料的安全性

（四）Windows 2000 的安全配置（重点）

理解：1．安全策略配置；2．文件保护

应用：其他有利于提高系统安全性的设置

第六章　Web 安全

一、学习目的与要求

本章主要介绍与 Web 有关的问题，通过本章学习，考生应掌握 Web 服务的安全威胁、Web 服务器的安全漏洞、Web 服务器的安全配置、Web 客户安全性、SSL 原理及应用以及 SET 原理等内容。

二、考核知识点与考核目标

（一）Web 安全概述（一般）

识记：1．Web 服务；2．Web 服务面临的安全威胁

（二）Web 安全问题（重点）

识记：1．Web 安全服务器的安全漏洞；2．通用网管接口

理解：1．CGI 的安全性；2．ASP 与 Access 的安全性；3．Java 与 Javascript 安全性；4．Cookies 的安全性

（三）Web 服务器的安全配置（重点）

识记：基本原则

理解：Web 服务器的安全配置方法

（四）客户的安全（重点）

识记：1．防范恶意网页；2．隐私侵犯

（五）SSL 技术（重点）

识记：1．SSL 概述；2．SSL 体系结构

理解：基于 SSL 的 Web 安全访问配置

（六）安全电子交易----SET（重点）

识记：1．网上交易的安全需求；2．SET 概述

理解：SET 的双重签名机制

第七章　电子邮件安全

一、学习目的与要求

本章主要内容讲述电子邮件安全问题，通过学习，考生应该掌握电子邮件系统存在的主要安全问题、使用 PGP 进行邮件加密和签名、使用 Outlook Express 发送安全邮件的方法。

二、考核知识点与考核目标

（一）电子邮件系统原理（次重点）

识记：1．电子邮件系统简介；2．邮件网关

理解：SMTP 与 POP3 协议

（二）电子邮件系统安全问题（重点）

识记：1．匿名转发；2．电子邮件欺骗；3．E-mail 炸弹；4．垃圾邮件

（三）PGP（重点）

识记：PGP 定义

理解：1．PGP 的密钥管理；2．PGP 应用系统介绍

（四）Outlook Express 的安全功能（一般）

识记：S/MIME 协议

理解：Outlook Express 中的安全措施

应用：拒绝垃圾邮件

第八章　防火墙技术

一、学习目的与要求

本章主要介绍防火墙概念、分类、体系结构及有关产品，通过本章学习，考生应掌握防火墙定义及相关概念、包过滤与代理、防火墙的体系结构、分布式防火墙与嵌入式防火墙。

二、考核知识点与考核目标

（一）防火墙概述（重点）

识记：1．相关概念；2．防火墙的优点和缺点

理解：防火墙的作用

（二）防火墙技术分类（重点）

识记：1．包过滤技术；2．代理技术

理解：防火墙技术的发展趋势

（三）防火墙体系结构（重点）

识记：1．双重宿主主机结构；2．屏蔽主机结构；3．屏蔽子网结构

理解：防火墙的组合结构

（四）内部防火墙（重点）

识记：分布式防火墙

理解：嵌入式防火墙

应用：个人防火墙

（五）防火墙产品介绍（一般）

识记：1．FireWall-1；2．天网防火墙

第九章　计算机病毒与反病毒技术

一、学习目的与要求

本章介绍与计算机病毒以及反病毒技术相关的一些背景知识、基本原理和方法，通过本章的学习，考生应掌握计算机病毒的发展历史及危害、计算机病毒的基本特征和传播方式、病毒的结构、常用的反病毒技术和常见的病毒防范方法。

二、考核知识点与考核目标

（一）计算机病毒（重点）

识记：1．计算机病毒的历史；2．病毒的本质；3．病毒的分类；4．病毒的传播及危害

应用：病毒的命名

（二）几种典型病毒的分析（一般）

识记：1．CIH 病毒；2．宏病毒；3．蠕虫病毒

（三）反病毒技术（重点）

识记：反病毒技术的发展阶段

理解：高级反病毒技术

（四）病毒防范措施（重点）

识记：防病毒措施

理解：1．常用杀毒软件；2．在线杀毒；3．杀毒软件实例

第十章　网络攻防和入侵检测

一、学习目的与要求

本章主要讲述黑客和网络攻击的一些基础知识和常见的攻击手段和技术等，通过学习，要求考生了解黑客和网络攻击的基础知识，掌握口令攻击、端口扫描、网络监听、IP 欺骗、拒绝服务、特洛伊木马等攻击方式的原理、方法及危害；掌握入侵检测技术和入侵检测系统的原理，了解识别与防范各类攻击的方法，了解入侵检测工具。

二、考核知识点与考核目标

（一）网络攻击概述（重点）

识记：1．关于黑客；2．黑客攻击的步骤；3．网络入侵的对象

理解：1．主要的攻击方法；2．攻击的新趋势

（二）典型攻击方式（重点）

识记：口令攻击、扫描器、网络监听、IP 欺骗、拒绝服务、特洛伊木马、

入侵检测概述、入侵检测系统、入侵检测工具介绍。

理解：拒绝服务，IP 欺骗，口令攻击

第十一章　网络管理原理

一、学习目的与要求

本章主要介绍网络管理的基本概念、物流管理协议及其发展，通过本章学习，应掌握网络管理的概念、目标、功能和网络管理的标准，简单网络管理协议的体系结构、安全和实现，简单网络管理协议模型的发展，了解网络管理技术的新发展。

二、考核知识点与考核目标

（一）网络管理简介（重点）

识记：1．网络管理概述；2．网络管理的标准

理解：1．网络管理的功能；2．网络管理的方式

（二）简单网络管理协议（重点）

识记：1．SNMP 的管理模型；2．SNMP v1 的体系结构；3．SNMP v1 的安全机制

理解：1．SNMP v1 的实现问题；2．SNMP v2；3． SNMP v3；4．RMON

（三）网络管理技术的新发展（重点）

识记：网络管理技术的发展趋势

理解：基于 Web 的网络管理

应用：1．基于 CORBA 技术的网络管理；2．基于主动网的网络管理；3．基于专家系统的网络管理

第十二章　网络管理系统

一、学习目的与要求

本章主要介绍网络管理系统的概念，常用网络管理软件及其配置管理，通过本章学习，考生应该掌握网络管理平台、管理系统、管理体系的概念，了解 SNMP 在 Windows 2000、网络设备上的实现、了解 HP Open View 管理软件的管理功能和应用，了解 CA Unicenter TNG 软件的使用方法。

二、考核知识点与考核目标

（一）网络管理系统的结构（重点）

识记：网络管理平台的功能结构

理解：网络管理体系的结构

应用：网络管理系统的选择

（二）配置网络节点（重点）

理解：1．网络设备的配置；2．Windows 2000 下的 SNMP 服务

（三）网络管理软件（一般）

理解：1．HP OpenView NNM ；2．CISCO Works 2000；3．综合企业管理平台——Unicenter TNG。

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

1．指定教材：

网络安全与管理，戚文静，中国水利水电出版社，2008 年第 2 版

2．参考书目：

计算机网络管理与安全技术，李艇，高等教育出版社，2008 年版

计算机网络管理与安全技术，杜威，武汉大学出版社，2009 年版

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。

网络安全与管理课程对自学考生来说是一门较难的课程，该课程的知识面宽，需要考生具备计算机网络、高级程序设计语言、密码学等专业课程的基础知识。因此，考生在学习时必须了解各章的考试知识点，以及对各知识点的考核要求，

根据要求来掌握学习的深度和广度。

网络安全与管理课程内容涉及面较宽，自学考生在自学过程中应注意如下几个方面：

（1）根据考核要求中的能力层次，在全面系统学习的基础上掌握重点概念和重点问题，如数据结构的基本特性、线性结构、树结构等，注意各章内容之间的内在联系。

（2）本课程的自学考试大纲是自学本课程的主要依据。在自学本课程前应先通读大纲，了解课程的要求，获得课程完整的概况。在开始自学某一章时，先阅读大纲，了解该章的课程内容，考核知识点和考核要求，在自学过程中有的放矢。

（3）阅读指定教材时，要求吃透每个考核知识点。对基本概念要做到深刻理解，对基本原理要弄清弄懂，对基本方法要熟练掌握。

（4）重视每章末的习题的作用，自学考生需要多做习题，可以帮助考生尽快地达到自考大纲的要求，并可以检查学习掌握知识的程度。

（5）本课程是一门实践性较强的课程，自学考生在自学过程中必须注意理论联系实际，按实验的目的、要求和内容认真做好实验。建议实验与课程自学过程同步进行。

（6）自学考生在自学时要注意基本能力的培养，即系统分析和综合能力，分析问题和理解知识的能力，抓住重点阐述问题的能力，以及实验能力等。

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 3 学分，建议总课时 54 学时，其中助学课时分配如下：

章　次	内　容	学　时
第一章	网络安全概述	2
第二章	网络操作命令及协议分析	4
第三章	密码学基础	4
第四章	密码学应用	4

第五章	操作系统的安全机制	4
第六章	Web 安全	4
第七章	电子邮件安全	6
第八章	防火墙技术	6
第九章	计算机病毒与反病毒技术	6
第十章	网络攻防和入侵检测	6
第十一章	网络管理原理	4
第十二章	网络管理系统	4
合　　计		54

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 50%、“理解”为 40%、“应用”为 10%。

3．试题难易程度应合理：易、较易、较难、难比例为 2：3：3：2。

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、判断题、填空题、名词解释题、简答题、论述题。

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．在以下人为的恶意攻击行为中，属于主动攻击的是

A．数据篡改及破坏　　B．数据窃听

C．数据流分析　　D．非法访问

二、判断题（本大题共■小题，每小题■分，共■分）

判断下列各题正误，正确的用“√”表示，错误的用“×”表示。

1．完整性是网络信息安全的特征之一。

三、填空题（本大题共■小题，每小题■分，共■分）

1．信息安全的特征为：完整性、保密性、可用性、_____、可控性。

四、名词解释（本大题共■小题，每小题■分，共■分）

1．计算机病毒

五、简答题（本大题共■小题，每小题■分，共■分）

1．请阐述 OSI-RM 的分层结构。

六、论述题（本大题共■小题，每小题■分，共■分）

1．从病毒的结构解释病毒的传播和感染机制。