高纲 4269

江苏省高等教育自学考试大纲

03344　信息与网络安全

南京理工大学编（2024 年）

Ⅰ　课程性质与课程目标

一、课程性质和特点

《信息与网络安全》课程是江苏省高等教育自学考试信息管理与信息系统专业（专升本）的必修课，该课程是信息管理与信息系统专业课程体系中的基础课程之一。其任务是培养信息管理与信息系统专业人才，掌握信息安全技术的理论知识和实际技能。

本课程是一门实操性很强的专业课，既向学生传授网络安全与管理的理论基础，又能在信息领域学习中产生实际应用价值。课程侧重于网络安全与管理的理论和方法体系，同时兼顾一定的实际问题分析与应用的掌握。因此考生在掌握相关理论与方法的同时，一定要加强实际应用问题分析能力的培养，考生应当考察实际的各类网络安全与管理应用，注重解决实际问题，以便考生能把课程中所学的方法、原理应用到实际的网络安全与管理中。

二、课程目标

《信息与网络安全》课程是一门集知识和技能于一体，实践性很强的课程，课程设置的目标是鼓励考生：

1. 掌握网络安全与管理的理论和方法体系，包括网络安全的基本概念，网络安全应用技术，网络安全管理工具，网络安全等级保护 2.0 标准，使学生能够综合运用所学知识、技术，提高网络信息安全方面的实践能力。

2. 掌握相关的计算机知识，包括：计算机基础理论、操作系统、网络技术、网络安全工具、密码学等。

3. 熟悉网络安全与管理的业务规范和操作技能，通过对网络安全所涉及的理论和技术的系统学习，实验演练，具备承担网络安全与管理的基本业务素质和知识结构。

三、与相关课程的联系与区别

学习本课程应具备的一定的计算机操作能力，了解计算机网络基本知识。

四、课程的重点和难点

本课程的重点在于，首先，网络信息安全是建立在网络基础知识之上的，学生需要对网络体系结构、协议、设备等有深入的了解，才能够更好地理解安全机制和技术。其次，学生需要掌握安全的基本概念，包括机密性、完整性、可用性

等，以及安全策略的制定与实施。再次，学生需要了解常见的网络威胁和攻击类型，包括病毒、蠕虫、木马等，以及其工作原理和防范措施。最后，学生还需要熟悉各种安全技术的应用，如入侵检测与防御、加密技术、防火墙配置等，以及在实际环境中的部署和管理。

本课程的难点在于，首先，许多安全技术涉及复杂的算法和协议，学生需要具备较强的技术功底和逻辑思维能力，才能够理解和应用这些技术。其次，网络威胁形势不断变化，新的攻击手段不断出现，学生需要具备持续学习的能力，及时了解最新的安全漏洞和威胁。再次，虽然理论知识重要，但在真实环境中的实践经验同样重要。学生需要通过案例分析和实验练习，加深对安全技术的理解和掌握。最后，网络安全工作需要进行全面的风险评估和管理，学生需要了解风险评估方法和工具，以及如何根据评估结果制定有效的安全策略。

II　考核目标

本大纲在考核目标中，按照识记、领会、简单应用和综合应用四个层次规定其应达到的能力层次要求。四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网络安全与管理的基本理论和基础知识（如定义、分类、技术、方法、技巧、模式、步骤、效果评价、特点等），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网络安全与管理基础知识的内涵及外延，理解网络安全的基本概念、应用技术、管理工具的使用以及等级保护2.0标准的解读；理解相关知识的区别和联系，并能根据考核的不同要求对网络安全与管理问题进行分析，做出正确的判断、解释和说明。

简单应用：要求考生能够根据已知的知识和网络安全管理工具使用的需求，对网络信息安全实践方面的问题进行分析，加强信息安全等级保护，综合运用各种网络安全技术以达到全面保护网络的要求。

综合应用：要求考生能够面对具体、实际的网络安全管理问题，能探究解决问题的方法，分析网络安全的具体解决方案，综合运用网络安全应用技术、网络安全管理工具，制定网络安全与管理策略，并进行实际效果的分析。

Ⅲ　课程内容与考核要求

第一章　网络安全概述

一、学习目的与要求

通过本章学习，考生应当了解互联网基础知识；理解威胁网络安全的因素，常见网络攻击形式；掌握常用网络密码安全保护技巧；重点掌握个人数据信息面临的网络威胁，网络攻击分类，常见网络攻击形式等。

二、考核知识点与考核要求

（一）互联网介绍

领会：①互联网的影响；②互联网的意义；③我国互联网的规模与使用情况。

（二）网络安全介绍

识记：①网络安全的概念；②网络安全的重要性；③网络安全的种类。

（三）威胁网络安全的因素

识记：①黑客；②黑客的行为；③黑客攻击；④网络攻击分类；⑤常见网络攻击形式。

领会：①史上最危险的计算机黑客。

（四）我国互联网网络安全现状

识记：①恶意程序；②安全漏洞；③拒绝服务攻击；④网站安全；⑤云平台安全。

领会：①工业控制系统安全。

（五）个人数据信息面临的网络威胁

识记：①Cookie 的使用；②黑客的行为；③黑客攻击；④网络攻击分类；⑤常见网络攻击形式；⑥个人信息安全保护；⑦个人信息保护法。

领会：①利用木马程序侵入计算机；②钓鱼网站；③监视网络通信记录；④手机厂商侵犯隐私。

（六）常见网络安全技术简介

识记：①网络监控技术；②认证签名技术；③安全扫描技术；④密码技术；⑤防病毒技术；⑥防火墙技术。

（七）常用网络安全保护技巧

领会：①了解并掌握 10 类密码破解方法和政策。

（八）国家网络空间安全战略

识记：①机遇和挑战；②网络空间安全的目标；③网络空间安全的原则。

领会：①网络空间安全的战略任务。

（九）大数据技术下的网络安全

识记：①大数据技术的有关概念。

领会：①大数据技术背景下的网络安全问题。

（十）我国网络安全产业介绍

识记：①我国网路安全产业进展；②我国网络安全产业前景展望。

领会：①全球网络安全产业规模；②我国网络安全竞争力情况。

三、本章重点

重点：①个人数据信息面临的网络威胁；②网络攻击分类；

难点：①常见网络攻击形式。

第二章　网络监控原理

一、学习目的与要求

通过本章学习，考生应当了解网络监控软件，理解 Sniffer Pro 软件，同时能够掌握网路岗软件的应用，以及常用网络监控软件的使用。

二、考核知识点与考核要求

（一）网络监控介绍

识记：①为什么要进行网络监控；②网络监控的分类。

领会：①网络监控的主要目标。

（二）Sniffer 工具

识记：①Sniffer介绍；②Sniffer原理；③Sniffer的工作环境；④Sniffer攻击；⑤如何防御Sniffer攻击。

综合应用：①Sniffer 的应用。

（三）Sniffer Pro 软件

识记：①Sniffer Pro 软件简介；②Sniffer Pro 软件使用

（四）网路岗软件

识记：①网路岗的基本功能；

领会：①网路岗对上网的监控程度。

简单应用：①网路岗安装方式。

三、本章重点、难点

重点：①网路岗软件的应用。

难点：①常用网络监控软件的使用。

第三章　操作系统安全

一、学习目的与要求

通过本章学习，考生应当了解国际安全评价标准的发展及其联系；掌握计算机安全评价标准相关内容；掌握我国安全标准相关内容；掌握安全操作系统的基本特征，安全操作系统的基本特征及解决方案；掌握 Windows 操作系统安全的基本内容。

二、考核知识点与考核要求

（一）国际安全评价标准的发展及其联系

识记：①计算机安全评价标准；②欧洲安全评价标准；③加拿大评价标准；④美国联邦准则。

领会：①国际通用准则。

（二）我国安全标准简介

识记：①用户自主保护级；②系统审计保护级；③安全标记保护级；④结构化保护级；⑤访问验证保护级。

（三）安全操作系统的基本特征

识记：①最小特权原则；②访问控制；

领会：③安全审计功能。

简单应用：①安全隔离功能。

（四）Windows 操作系统安全

识记：①远程攻击 Windows 系统的途径；②取得合法身份后攻击手段；③Windows 安全功能；④Windows 认证机制；⑤Windows 文件系统安全。

领会：①Windows 加密机制；

简单应用：①Windows 备份与还原。

（五）Android 操作系统安全

识记：①Android 安全体系结构；②Liunx 安全性；③Android 应用安全。

简单应用：①文件系统许可/加密。

三、本章重点、难点

重点：①我国安全标准简介。

难点：①计算机安全评价标准；②Windows 操作系统安全。

第四章　密码技术

一、学习目的与要求

通过本章学习，考生应当了解密码体系；了解《中华人民共和国密码法》；掌握常用的对称密钥算法和非对称密钥密码体制；掌握数字签名与数字证书技术；熟悉 PGP 加密软件的使用。

二、考核知识点与考核要求

（一）密码学的发展历史

识记：①现代密码（计算机阶段）；②密码学在网络信息安全中的作用。

领会：①古典密码；②隐写术；③转轮密码机。

（二）密码学基础

识记：①密码学相关概念；②密码系统。

领会：①密码学的基本功能。

（三）密码体制

识记：①对称密钥密码体制；②常用的对称密钥算法；③非对称密钥密码体制。

领会：①常用的公开密钥算法。

综合应用：①查找资料，了解常用加密软件的使用。

（四）哈希（Hash）算法

识记：①哈希（Hash）算法的定义；②哈希（Hash）算法的特性。

领会：①典型的哈希（Hash）算法；②MD5 简介。

（五）PGP 加密软件

识记：①PGP 的技术原理；②PGP 的密钥管理。

（六）软件与硬件加密技术

识记：①软件加密；②硬件加密。

（七）数字签名与数字证书

识记：①数字签名的定义；②数字证书。

领会：①数字证书的分类。

（八）PKI 基础知识、认证机构（CA）

识记：①PKI 的基本组成；②PKI 的安全服务功能。

（九）认证机构

识记：①认证机构的功能；②CA 系统的组成。

领会：①国内 CA 现状。

（十）《中华人民共和国密码法》介绍

识记：①《密码法颁布的意义》；②《密码法》的主要内容。

领会：①PKI 应用及密码行业大有可为。

三、本章重点、难点

重点：①密码学基础、密码体制；②数字签名与数字证书。

难点：①PKI 基础知识、认证机构（CA）。

第五章　病毒技术

一、学习目的与要求

通过本章学习，考生应当掌握计算机病毒的定义、特点、分类，了解计算机病毒的发展史，掌握木马病毒和蠕虫病毒的防治，熟悉常用病毒检测技术。

二、考核知识点与考核要求

（一）病毒的基本概念

识记：①计算机病毒的定义；②计算机病毒的特点；③计算机病毒的分类；④计算机病毒的发展史；⑤其他的破坏行为。

领会：①计算机病毒的危害性；②知名计算机病毒简介。

（二）网络病毒

识记：①木马病毒的概念；②木马的种类；③木马病毒案例；④木马病毒的防治；⑤蠕虫病毒的概念；⑥蠕虫病毒案例；⑦蠕虫病毒的防治。

领会：①病毒、木马、蠕虫的比较；②网络病毒的发展趋势；

简单应用：①计算机防毒杀毒的常见误区。

（三）流氓软件

识记：①流氓软件的定义；②流氓软件的分类。

综合应用：①流氓软件的防治。

（四）计算机病毒发展趋势

识记：①移动终端安全问题；②云服务安全问题。

领会：①网络支付面临的安全形势。

（五）病毒检测技术

简单应用：①传统的病毒检测技术；

综合应用①基于网络的病毒检测技术。

三、本章重点、难点

重点：①计算机病毒的定义、特点、分类；②其他的破坏行为、计算机病毒的危害性。

难点：①木马病毒和蠕虫病毒的防治。

第六章　防火墙技术

一、学习目的与要求

通过本章学习，考生应当了解防火墙的技术发展历程，了解防火墙的功能及基本特性，了解防火墙的分类及防火墙关键技术，掌握防火墙的分类，掌握防火墙关键技术的配置过程。

二、考核知识点与考核要求

（一）防火墙概述

识记：①防火墙的功能；②防火墙的基本特性。

领会：①防火墙的主要优缺点。

（二）DMZ 简介

识记：①DMZ 的概念；②DMZ 网络访问控制策略。

综合应用：①DMZ 服务配置。

（三）防火墙的技术发展历程

识记：①第 1 代防火墙：基于路由器的防火墙；②第 2 代防火墙：用户化的防火墙；③第 3 代防火墙：建立在通用操作系统上的防火墙；④第 4 代防火墙：具有安全操作系统的防火墙。

（四）防火墙的分类

识记：①软件防火墙；②包过滤防火墙；③状态检测防火墙；④代理防火墙。

（五）防火墙硬件平台的发展

识记：①x86 平台；②ASIC 平台；③NP 平台。

（六）防火墙关键技术

识记：①访问控制；②NAT；③VPN。

（七）个人防火墙

识记：①个人防火墙的概念；②个人防火墙的功能、设置、安全记录。

领会：①常见的个人防火墙。

（八）下一代防火墙

识记：①下一代防火产品的特点。

领会：①下一代防火墙的功能。

三、本章重点、难点

重点：防火墙的基本特性、DMZ 简介；防火墙关键技术、访问控制、NAT、VPN。

难点：了解下一代防火墙。

第七章 无线网络安全

一、学习目的与要求

通过本章学习，考生应当掌握无线网络的分类、WLAN 技术，提高无线网络安全的方法，掌握无线网络安全的防范措施。

二、考核知识点与考核要求

（一）无线网络安全概述

识记：①无线网络的分类；②WLAN 技术；

领会：①无线网络安全的关键技术。

简单应用：①无线网络存在的安全隐患。

（二）WLAN 安全

领会：①WLAN 的访问控制技术；②WLAN 的数据加密技术。

简单应用：①WAPI 与 WiFi 的竞争。

（三）无线网络安全的防范措施

识记：①公共 WiFi 上网安全注意事项。

领会：①提高无线网络安全的方法。

三、本章重点、难点

重点：①无线网络的分类；②WLAN 技术。

难点：①无线网络安全的防范措施。

第八章　VPN 技术

一、学习目的与要求

通过本章学习，考生应当了解各种安全隧道协议，了解 VPN 技术及其应用，掌握 Hash 函数和数据完整性技术，掌握基于电子证书的公钥认证的使用，了解 IPSec 的好处，熟悉 VPN 技术应用案例。

二、考核知识点与考核要求

（一）VPN 概述

识记：①什么是 VPN；②VPN 的发展历程；③VPN 的基本功能。

领会：①VPN 特性。

（二）常用 VPN 技术

识记：①IPSec VPN；②SSL VPN；③MPLS VPN。

简单应用：①SSL VPN，IPSec VPN，MPLS VPN 的比较。

（三）VPN 采用的安全技术

识记：①隧道技术；②加密技术；

简单应用: ①密钥管理技术。

综合应用：①使用者与设备身份认证技术。

（四）VPN 的分类

识记：①内部网 VPN；②远程访问 VPN；③外联网 VPN。

（五）VPN 技术应用

识记：①大学校园网 VPN 技术要求。

领会：①某理工大学校园网 VPN 使用指南。

三、本章重点、难点

重点：①VPN 的基本功能；②VPN 所需的安全技术；③VPN 的分类；④基于电子证书的公钥认证；Hash 函数和数据完整性。

难点：①加密和数据可靠性、密钥管理。

第九章　电子商务安全

一、学习目的与要求

通过本章学习，考生应当了解互联网安全的基本概念，了解电子商务安全分类，了解电子商务安全分类、安全策略和综合安全，掌握客户端的安全，掌握服务器的安全。

二、考核知识点与考核要求

（一）互联网安全概述

识记：①风险管理；②电子商务安全分类。

领会：①安全策略和综合安全。

（二）客户端的安全

识记：①Cookie；②Java 小程序；③JavaScript；④ActiveX 控件。

领会：①图像文件与插件；②数字证书；③信息隐蔽。

（三）通信的安全

识记：①对保密性的安全威胁；②对完整性的安全威胁；③对即需性的安全威胁；④对互联网通信信道物理安全的威胁；⑤对无线网的威胁；⑥加密。

领会：①用哈希函数保证交易的完整性；②用数字签名保证交易的完整性；③保证交易传输。

（四）服务器的安全

识记：①对 WWW 服务器的安全威胁；②对数据库的安全威胁；③对其他程序的安全威胁；④对 WWW 服务器物理安全的威胁。

领会：①访问控制和认证。

（五）电子商务安全实例

领会：①保证数据安全的工具。

综合应用：①电子商务安全实例。

三、本章重点、难点

重点：①客户端的安全、服务器的安全。

难点：①电子商务安全实例。

第十章　漏洞扫描技术

一、学习目的与要求

通过本章学习，考生应当了解漏洞的概念、定义、分类，掌握漏洞扫描原理、漏洞扫描过程掌握漏洞扫描工具的使用，掌握网络漏洞扫描技术分析方法，掌握传统的网络安全扫描技术。

二、考核知识点与考核要求

（一）漏洞的概念

识记：①漏洞的定义；②漏洞的分类；③漏洞与环境和时间的关系。

领会：①漏洞信息发布。

（二）漏洞扫描

识记：①漏洞扫描原理；②漏洞扫描过程。

（三）漏洞扫描工具

识记：①国外常用漏洞扫描工具简介；②国内常用漏洞扫描工具简介。

（四）网络漏洞扫描

识记：①网络漏洞扫描的意义；②网络漏洞扫描分析。

领会：①传统的网络安全扫描技术；②非入侵式网络安全扫描技术。

（五）数据库漏洞扫描

识记：①概述；②数据库安全产品分类；③数据库扫描系统特性。

领会：①数据库扫描系统介绍。

（六）Web 漏洞扫描

识记：①基本概念；②十大常见的 Web 漏洞。

简单应用：①常用的 Web 漏洞扫描工具。

（七）Android 漏洞扫描

识记：①Android 常见风险及预防；②Android 漏洞扫描工具。

领会：①Android 常见漏洞。

三、本章重点

重点：①漏洞的扫描和检测。。

难点：①各类漏洞分析。

第十一章　入侵检测与防御

一、学习目的与要求

通过本章学习，考生应当了解入侵检测与防御基本概念，了解入侵检测系统和方法，了解 IPS 设备，掌握 IDS 与 IPS 的部署。

二、考核知识点与考核要求

（一）基本概念

识记：①入侵检测系统；②入侵防御系统。

领会：①入侵防御系统的作用。

（二）入侵检测系统

识记：①系统功能；②入侵检测系统评价；③入侵监测系统分类；④检测原理；⑤入侵检测模型。

领会：①入侵检测步骤；②入侵检测系统与防火墙。

（三）入侵检测方法

识记：①异常检测方法；②误用检测方法。

领会：①其他检测方法。

（四）IDS 与 IPS 的部署

识记：①IDS 的部署；②IPS 的部署。

领会：①联合部署；②分布式部署。

（五）IPS 设备介绍

识记：①深信服 NIPS；②网神 Seclps3600；③天融信 TopIDP。

（六）问题与展望

识记：①存在问题。

领会：①发展方向。

（七）Android 漏洞扫描

识记：①Android 常见风险及预防；②Android 漏洞扫描工具。

领会：Android 常见漏洞。

综合应用: ①使用工具检测漏洞

三、本章重点、难点

重点：①入侵检测系统；②入侵检测方法；③IDS 与 IPS 的部署。

难点：①IPS 设备介绍。

第十二章　网络安全等级保护 2.0 标准

一、学习目的与要求

通过本章学习，考生应当了解等级保护发展历程，掌握安全通用要求的内容，掌握安全扩展要求的内容。

二、考核知识点与考核要求

（一）等级保护发展历程

识记：①等级保护 1.0 时代发展历程；②等级保护 2.0 时代发展历程。

领会：①等级保护 2.0 特点和变化。

（二）安全通用要求的内容

识记：①安全通用要求基本分类；②技术要求。

领会：①管理要求。

（三）安全扩展要求的内容

识记：①云计算安全扩展要求；②移动互联安全扩展要求。

领会：①物联网安全扩展要求；②工业控制系统安全扩展要求。

三、本章重点、难点

重点：①等级保护发展历程；②安全通用要求的内容。

难点：①安全扩展要求的内容。

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

课程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。

课程自学考试大纲明确了课程学习的内容以及深广度，规定了课程自学考试的范围和标准。因此，它是编写自学考试教材和辅导书的依据，是社会助学组织进行自学辅导的依据，是考生学习教材、掌握课程内容知识范围和程度的依据，也是进行自学考试命题的依据。

二、课程自学考试大纲与教材的关系

课程自学考试大纲是进行学习和考核的依据，教材是学习掌握课程知识的基

本内容与范围，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。大纲与教材所体现的课程内容应基本一致；大纲里面的课程内容和考核知识点，教材里一般也要有。反过来教材里有的内容，大纲里就不一定体现。

三、关于自学教材

本课程使用教程为：《网络安全与管理》（第 3 版），石磊，赵慧然，肖建良主编，清华大学出版社，2021 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，在各章的基本要求中也指明了各章内容的重点和难点。

本课程以掌握网络安全知识为目的，以网络安全工具使用为重点，以理论讲述为基础的系统性、应用性较强的网络安全基础课程。包括网络监控技术、密码技术、病毒防御技术、防火墙技术、入侵检测技术、VPN 技术、无线网络安全技术、电子商务安全技术、漏洞扫描技术、入侵检测与防御，及其它的安全服务和安全机制策略。自学考试主要是通过个人自学、教师辅导、社会助学和国家考试来考核考生掌握专业知识和能力的方法。考生应根据自己的特点，找出适合自己的学习方法，此外，考生在自学过程中，应注意以下几点：

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.本课程内容涉及网络安全与管理的各个方面，知识、范围比较广泛，全书是一个整体，但各章之间又有相对独立性。考生应首先全面系统地学习各章的内容，深刻领会网络安全与管理中的理论知识；其次，要注意各章之间的联系；然后，在全面系统的基础上掌握重点，有目的地深入学习重点章节，但切忌在没有了解全貌的情况下孤立地去抓重点，押题目。

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。

5.注意将网络安全与管理理论与实践应用相结合。考生应明白，本课程从网络安全的各个方面进行了基本的介绍，这些介绍主要包括各种技术的概念、分类、原理、特点等知识，对于复杂而枯燥的算法和理论研究没有详细介绍，通过对这些知识的学习理解网络安全体系中各部分之间的联系。在学习过程中切忌死记硬背，而应当尽可能多上网，观察、分析和研究实际。本课程的教学内容不仅完全覆盖课程拟达成的具体目标，同时，根据计算机类专业人才培养总体目标，以及课程所面向学生特点，课程内容还涉及计算机网络、密码学、网络管理等内容，旨在培养知识交叉应用、沟通交流等综合工程能力。

五、应考指导

1.如何学习

很好的计划和组织是你学习成功的法宝。如果你正在接受培训学习，一定要跟紧课程并完成作业。为了在考试中作出满意的回答，你必须对所学课程内容有很好的理解。使用“行动计划表”来监控你的学习进展。你阅读课本时可以做读书笔记。如有需要重点注意的内容，可以用彩笔来标注。如：红色代表重点；绿色代表需要深入研究的领域；黄色代表可以运用在工作之中。可以在空白处记录相关网站，文章。

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。回答所提出的问题。要回答所问的问题，而不是回答你自己乐意回答的问题！避免超过问题的范围。

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。

4.如何克服心理障碍

这是一个普遍问题!如果你在考试中出现这种情况，试试下列方法：使用“线索”纸条。进入考场之前，将记忆“线索”记在纸条上，但你不能将纸条带进考场，因此当你阅读考卷时，一旦有了思路就快速记下。按自己的步调进行答卷。为每个考题或部分分配合理时间，并按此时间安排进行。

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，明确本课程与其它课程不同的特点和学习要求，对考生进行切实有效的辅导，引导他们防止自学中的各种偏向，把握社会助学的正确方向。

2.要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，掌握全部考核内容和考核知识点，并在此基础上在突出重点。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

1.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。因此，课程自学考试大纲中所规定的考试内容是以分解为考核知识点的方式给出的。由于各知识点在课程中的地位、作用以及知识自身的特点不同，自学考试将对各知识点分别按四个能力层次确定其考核要求。

2.本大纲在考核目标中，按照识记、领会、简单应用和综合应用四个层次要求考生掌握，四个能力层次是递进关系。

3.课程分为四个部分：网络安全的基本概念、网络安全应用技术、网络安全管理工具、网络安全等级保护 2.0 标准等。本课程以掌握网络安全知识为目的，以网络安全工具使用为重点，以理论讲述为基础的系统性、应用性较强的网络安全基础课程。包括网络监控技术、密码技术、病毒防御技术、防火墙技术、入侵

检测技术、VPN 技术、无线网络安全技术、电子商务安全技术、漏洞扫描技术、入侵检测与防御，及其它的安全服务和安全机制策略。考试试卷中四个部分所占的比例大约分别为：20%、25%、30%、25%。

八、关于考试命题的若干规定

本课程的命题考试，应根据本大纲规定的考试内容和考核目标来确定考试范围和考核要求，按大纲规定试题中主观性题和客观性题的比例来组配试卷，适当掌握试题的内容覆盖面、能力层次和难易度。

1.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。

2.命题不应有超出大纲中考核知识点范围的题目，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。

3.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 20%，领会占 30%，简单应用占 30%，综合应用占 20%。

4.试题要合理安排难度结构。试题难易可分为易、较易、较难、难四个等级。每份试卷中，不同难易试题的分数比例一般为：较易占 50%，较难占 30%，难 20%。注意，试题的难易度与能力层次不是一个概念，在各能力层次上都会存在不同难度的问题。

5.试卷的题型有：单项选择题、填空题、名词解释、简答题、论述题。在命题工作中必须按照本课程大纲中所规定的题型命制，考试试卷使用的题型可以略少，但不能超出本课程对题型规定。

6.本课程考试方法采用闭卷笔试，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。不可携带计算器。

附录　题型举例

一、单项选择题

1．计算机病毒通常是（　　）

A．一条命令　　B．一个文件

C．一个标记　　D．一段程序代码

参考答案：　D

二、填空题

1．基于密码体制的_____具有防否认功能，同样具有法律效力，可使人们遵守数字领域的承诺。

参考答案：　数字签名

三、名词解释

1.广告软件

参考答案：是指未经用户允许，下载并安装在用户计算机上；或与其他软件捆绑，通过弹出式广告等形式牟取商业利益的程序。

四、简答题

1．简述传统的病毒检测技术。

参考答案：

（1）程序和数据完整性检测技术

（2）病毒特征码检测技术

（3）启发式规则（或广谱特征码）病毒检测技术

（4）基于操作系统的监视和检测技术

（5）传统虚拟机病毒检测技术。

五、论述题

1．试述误用入侵检测系统中常用的检测方法。

参考答案：

（1）模式匹配法。通过把收集到的信息与网络入侵和系统误用模式数据库中的已知信息进行比较，从而对违背安全策略的行为进行标识。

（2）专家系统法。该方法的思想是把安全专家的知识表示成规则知识库，再用推理算法检测入侵。

（3）基于状态转移分析的检测法。该方法的基本思想是将攻击看成一个连续的、分步骤的并且各个步骤之间有一定的关联的过程。

（4）基于键盘监控的误用入侵检测。该方法是假定入侵活动与某种确定的击键序列模式相对应，通过监控对象的击键模式并把该模式和入侵模式进行对比以发觉入侵行为。

（5）基于条件概率的误用入侵检测。该法将入侵方式对应一个事件序列，然后通过观测事件发生的情况推测入侵的出现。