NTC.ORG.CN 工业和信息化部全国网络与信息技术培训考试项目(NTC)指定教材

网络与信息安全专业指定教材

Network and information security

网络与信息安全

胡 铮 主编

科学出版社

工业和信息化部全国网络与信息技术培训考试项目（NTC）
网络与信息安全专业指定教材

网络与信息安全

胡　铮　主编

科学出版社
北　京

内 容 简 介

本书是工业和信息化部全国网络与信息技术培训考试项目（NTC）网络与信息安全专业指定教材。网络与信息安全是一门涉及计算机科学、网络技术、网络安全技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性科学。网络与信息安全问题在许多国家已经引起了普遍关注，成为当今信息技术的一个重要研究课题。本书利用通俗易懂的语言阐述了网络所涉及的安全问题，主要内容包括第 1 篇（事前预防）、第 2 篇（事中监测与治理）和第 3 篇（事后恢复）三个部分。第 1 篇内容包括网络安全概述、操作系统安全常识、病毒知识介绍、数据安全技术介绍和网络安全法律法规；第 2 篇内容包括防火墙技术、黑客攻击与入侵检测、虚拟专用网、网络通信安全和 Web 的安全；第 3 篇内容包括数据备份技术和安全恢复技术。

本书不仅适合各类院校及培训机构学生使用，同时也适合于任何对网络与信息安全感兴趣的读者。

图书在版编目(CIP)数据

网络与信息安全/胡铮主编. —北京：科学出版社，2011

（工业和信息化部全国网络与信息技术培训考试项目（NTC）·网络与信息安全专业指定教材）

ISBN 978-7-03-030626-5

Ⅰ.①网… Ⅱ.①胡… Ⅲ.①计算机网络-计算机安全-教材

Ⅳ.①TP 393.08

中国版本图书馆 CIP 数据核字（2011）第 049125 号

责任编辑：赵丽欣 陈晓萍 / 责任校对：刘玉靖

责任印制：吕春珉 / 封面设计：东方人华平面设计部

科学出版社出版

北京东黄城根北街 16 号

邮政编码 100717

http://www.sciencep.com

铭浩彩色印装有限公司 印刷

科学出版社发行 各地新华书店经销

*

2011 年 6 月第 一 版 开本：787×1092 1/16

2011 年 6 月第一次印刷 印张：18

印数：1—3 000 字数：429 000

定价：32.00 元

（如有印装质量问题，我社负责调换<骏杰>）

销售部电话 010-62142126 编辑部电话 010-62135517-8003

编 委 会

前　言

互联网的迅猛发展已经深刻地影响到国家的政治、经济、军事、文化等各个领域，与此同时，互联网的开放性和安全漏洞所带来的安全风险也给互联网的健康发展带来了不可忽视的影响。网络与信息安全问题不仅给相关单位及网民带来不便，而且已经威胁到国家的信息安全和经济发展。

随着信息化在我国的不断深入和发展，信息技术和网络给社会的经济、科教、文化和管理等各个方面注入了新的活力，对信息化人才的培养与评估不断提出新的要求。建立一个技术领先、既广泛涉及多厂商产品又保持内容中立的政府认证品牌成为我国信息化发展的当务之急。

为深入贯彻落实科学发展观，坚持走中国特色新型工业化道路，加快通信技术产业的发展和应用，同时为贯彻落实国家关于网络与信息技术发展及加强职业教育工作的指示精神，促进我国此类技术领域人才建设，工业和信息化部有关部门推出了全国网络与信息技术培训考试项目（NTC），网络与信息安全项目是NTC的子项目及组成部分。

NTC 项目是由工业和信息化部中国电子信息产业发展研究院与工业和信息化部通信行业职业技能鉴定指导中心联合共建。NTC 项目由全国网络与信息技术培训考试管理中心（NTC-MC）负责管理及运营，同时由国信高新技术培训中心（工业和信息化部有关部门批准设立的信息技术及游戏动漫培训考试机构）负责具体的运营工作，项目面向社会、各类院校、相关行业等，培养应用型、管理型信息技术复合型人才。学员考核通过后颁发工业和信息化部职业技能水平证书，作为职业技能水平的凭证及从事相关岗位的任职依据。

由于信息技术发展迅速，网络安全的相关技术在不断推陈出新，本书将从网络安全的事前预防（第 1 篇）、事中监测与治理（第 2 篇）和事后恢复（第 3 篇）三个层面，采用通俗易懂的语言，对网络与网络安全的各个方面进行阐述。

第 1 篇内容主要是对网络安全相关知识的介绍，包括网络安全概述、操作系统安全常识、病毒知识介绍、数据安全技术介绍和网络安全法律法规；第 2 篇内容主要是关于网络运行过程中的相关安全技术，包括防火墙技术、黑客攻击与入侵检测、虚拟专用网、网络通信安全和 Web 的安全；第 3 篇内容主要是关于在网络安全事故发生后如何恢复的技术，包括数据备份技术和安全恢复技术。具体内容如下：

第 1 章是网络安全概述，包括网络安全简介、网络安全面临的威胁、网络出现安全威胁的原因、网络安全机制。

第 2 章是操作系统安全常识，包括安全等级标准、漏洞、Windows Server 2003 系统安全、UNIX 系统安全、Linux 系统安全、Windows XP 系统安全及 Windows 7 系统安全。

第 3 章是病毒知识介绍，包括计算机病毒简介、网络病毒及其防治、典型病毒介绍及常用杀毒软件介绍。

第 4 章是数据安全技术介绍，包括数据加密及数据压缩。

第 5 章是网络安全法律法规，包括与网络有关的法律法规、网络安全管理的有关法

律和其他法律规范。

第 6 章是防火墙技术，包括防火墙简介、防火墙的类型、防火墙配置、防火墙系统、防火墙的选购和使用及防火墙产品介绍。

第 7 章是黑客攻击与入侵检测，包括黑客常用的攻击方法和防范措施、入侵检测响应与追踪。

第 8 章是虚拟专用网，包括 VPN 概述和 VPN 的配置实现。

第 9 章是网络通信安全，包括网络通信的安全性、网络通信存在的安全威胁、调制解调器的安全及 IP 安全。

第 10 章是 Web 的安全，包括 Web 技术简介、Web 的安全需求、Web 服务器安全策略、Web 浏览器安全策略及 Web 站点安全八要素。

第 11 章是数据备份技术，包括数据完整性、容错与网络冗余及网络备份系统。

第 12 章是安全恢复技术，包括网络灾难、安全恢复的条件、安全恢复的实现及安全恢复案例。

本书由胡铮任主编，参与编写人员有林鹏、孙蔚敏、刘占山、滕伟、马亮、童晓民、陈耿、王连宝、温安顺、苏红、谢赞福、高俊文、顾巧论、甘宏、张慧丽、彭英慧、申莉莉、蔡振山等。

在编著本书过程中，我们得到了工业和信息化部中国电子信息产业发展研究院、工业和信息化部通信行业职业技能鉴定指导中心、全国网络与信息技术培训考试管理中心（NTC-MC）、全国网游动漫学院项目管理办公室（GCC-MO）的大力支持，在此一并表示感谢。

在编写本书过程中，我们参考了大量书籍，在此对这些书的编著者表示感谢。

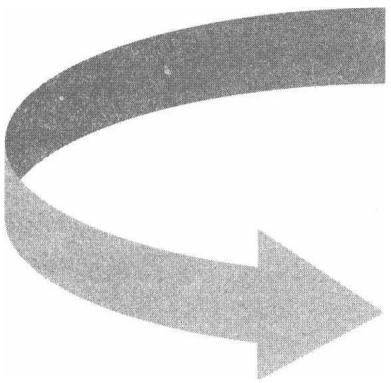
由于编者水平有限，书中错误和疏漏之处在所难免，希望读者和各位专家批评指正。

目　录

第1篇　事 前 预 防

第 2 篇 事中监测与治理

第 3 篇 事 后 恢 复



第 1 篇

事 前 预 防

第1章 网络安全概述

知识点

- 网络安全的定义
- 网络面临的安全威胁
- 网络出现安全威胁的原因
- 网络的安全机制

难点

- 网络安全威胁产生的原因

要求

熟练掌握以下内容：

- 网络安全的定义
- 网络面临的各种安全威胁
- 网络的安全机制

了解以下内容：

- 产生网络安全威胁的原因

随着网络技术的不断发展，网络在人们的生活中已经占有一席之地，给人们的生活带来了方便。然而，网络也不是完美无缺的，给人们带来惊喜的同时，也带来了威胁。计算机犯罪、黑客、有害程序和后门等严重威胁着网络的安全。目前，网络安全问题在许多国家已经引起了普遍关注，成为当今网络技术的一个重要研究课题。

1.1 网络安全简介

网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性科学。

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，确保系统能连续、可靠、正常地运行，网络服务不中断。网络安全从其本质上来讲就是网络上的信息安全。从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。

（1）保密性：信息不泄露给非授权用户。

（2）完整性：数据未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。

（3）可用性：可被授权实体访问并按需求使用的特性，即当需要时能否存取所需的信息。例如，网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。

（4）可控性：对信息的传播及内容具有控制能力。网络安全包括物理安全、逻辑安全、操作系统安全、联网安全。

1.1.1 物理安全

物理安全是指用来保护计算机硬件和存储介质的装置和工作程序。物理安全包括多方面的内容。

1. 防盗

像其他的物体一样，计算机也是偷窃者的目标，如盗走光驱、主板等。计算机偷窃行为所造成的损失可能远远超过计算机本身的价值，因此必须采取严格的防范措施，以确保计算机设备不会丢失。

2. 防火

计算机机房发生火灾一般是由于电气原因、人为事故或外部火灾蔓延引起的。电气设备和线路可能因为短路、过载、接触不良、绝缘层破坏或静电等原因引起电打火而导致火灾。人为事故是指由于操作人员不慎、吸烟、乱扔烟头等，使充满易燃物质（如纸片、磁带、胶片等）的机房起火，当然也不排除人为故意放火。外部火灾蔓延是因外部房间或其他建筑物起火而蔓延到机房而引起火灾。

3. 防静电

静电是由物体间的相互摩擦、接触而产生的，计算机显示器也会产生很强的静电。静电产生后，由于未能释放而保留在物体内，会有很高的电位（能量不大），从而产生静电，放电火花，造成火灾；还可能使大规模集成电器损坏，这种损坏可能是不知不觉造成的。