王 达 编著
飞思科技产品研发中心 监制

网管第1课
——计算机与网络安全

- 定位于准网管、初级网管和广大网络爱好者
- 提供教学课件下载与同步实践，强化教学效果
- Step-by-Step教学模式，实用性强，直观易懂
- 无复杂理论，纯实例操作和经验介绍，易教易学

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

王 达 编著
飞思科技产品研发中心 监制

网管第一课

——计算机与网络安全

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

本书共 8 章，分别从个人计算机和计算机网络的角度介绍了各种安全防护技术及其应用。其中主要包括计算机病毒、木马和恶意软件的清除和预防，IE 浏览器、Windows 防火墙、第三方个人防火墙和主流应用软件的安全防护设置，系统漏洞扫描与修复，黑客攻击及其预防方法，网络防火墙技术及其应用，IDS 和 IPS 技术及其应用，文件加密和数字签名技术及应用等。全书形成了一个比较完整的计算机和网络防护体系。

本书的主要特点是结合了当前大量实际安全防护应用需求，介绍了大量实际可行的方案配置，是计算机和网络安全入门自学和培训的最佳选择。

图书在版编目（CIP）数据

网管第一课：计算机与网络安全 / 王达编著.—北京：电子工业出版社，2008.1
ISBN 978-7-121-05343-6

Ⅰ. 网… Ⅱ.王… Ⅲ.①电子计算机－安全技术②计算机网络－安全技术 Ⅳ.TP309 TP393.08

中国版本图书馆 CIP 数据核字（2007）第 175315 号

责任编辑：王树伟 黄瑞友
印　　刷：北京四季青印刷厂
装　　订：涿州市桃园装订有限公司
出版发行：电子工业出版社
　　北京海淀区万寿路 173 信箱　邮编：100036
开　　本：787×1092　1/16　印张：19.75　字数：505.6 千字
印　　次：2008 年 1 月第 1 次印刷
印　　数：6 000 册　　定价：29.80 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

心存征服网络技术信念的你
怀抱投身网管生涯热忱的你
是否急需有人帮你快速上手
是否渴望早日成为职业网管

INTRODUCTION

出版说明

——“网管第一课”，职业网管成长的摇篮！

网管员是许多人梦寐以求的职业之一，同时也是一个需要具备足够知识、技能储备的工作岗位。随着网络信息化建设在各行各业的普及，网管员的重要性日益突显。一个企业从网络系统的选型与构建，网络设备的管理与维护，应用服务的配置与优化，到安全防护的规划与实施等方方面面，都由这一人群来主导和完成。与此同时，网络管理水平也已逐渐成为直接影响网络性能、安全、效率等指标的关键因素，网管员的工作内容由原来的机房维护发展为今天的网络配置和日常性能维护，网络功能的软、硬件配合和拓展，以及接入互联网的安全防范等。这使得网管员的工作越来越复杂，难度越来越大。由此可见，成为网管员的先决条件就是技术要过关。公司最重要的数据资产和网络服务设施掌握在网管手上，不懂技术就无法做到高效而稳定的服务和保障。因此，不管是立志在网管岗位上开创事业的学生，还是决定转行从事网管职业的在职者，都要为此目标而积极地去学习和准备。其实，担任网管工作并非遥不可及的梦想，具备一定程度的电脑操作基础，再加上必要的自学和培训，就完全可以为自己赢得机会。

网管岗位需求的旺盛，带动了网管类图书出版的热潮，每年都会有大量的相关图书投放市场。种类繁多，品质难免参差不齐，这给广大网络技术学习者造成很大困惑。有鉴于此，我们在网管技术类图书的策划和出版过程中，始终严把质量关，陆续推出多套口碑上佳的畅销丛书。其中，《网管员必读》系列图书不仅销量位居国内同类图书首位，而且还获得“2005年度版权输出优秀图书奖”、“2006年度全行业畅销品种奖”等全国或全行业图书大奖。为保证品质，本系列图书《网管第一课》主要由《网管员必读》、《网络工程师必读》等畅销图书的作者王达亲自执笔，力争为广大网络技术院校师生献上一套高质量的精品图书。

《网管第一课》策划初衷

目前，国内的高校和培训网管类教材比较混乱，质量良莠不齐，很难找到一套系统、实用的优质教材。各高校和培训机构现在采用的网管教学或培训教材，只能由零售图书中不同作者，甚至不同出版社出版的单行本拼凑而成。这不仅使各本书之间可能存在知识点和技能训练的重复，而且还不能保证知识点和技能训练的系统性和全面性。此外，受限于高质量培训教材的匮乏，许多高校和培训机构的课程安排也不尽合理。一方面，课程设计没有按照学生或学员今后所从事的实际网络管理工作的需求来安排，所选教材严重缺乏实用性，更看不到能全面体现当前主流网络技术和热点应用的图书；另一方面，有的课程仍

在教授非常陈旧的知识点，选用操作系统的版本也远远落后于主流版本。正是由于当前的培训市场急需这样一套符合当前技术现状与教学需求的网管教材，飞思科技产品研发中心与王达老师共同精心打造了《网管第一课》这一全新的系列。

《网管第一课》图书定位

《网管第一课》系列图书主要面向高等院校和培训机构网络技术相关专业的师生，或新近转入网管行业的准网管和初级网管朋友。对于初涉网络管理这一技术领域的初级网管朋友们来说，最急需解决的问题就是对网络基本认识和实际动手能力的提高。本系列图书也正是基于这一需求来规划选题和组织内容的。系列中除了第一本《网管第一课——计算机网络原理》一书外，其他各本基本上是直接针对实际网络管理工作需求来编写的。立足实用是我们一贯的策划思路与出版风格，也是诸多高校和培训机构选用教材的首要标准。由于市面上现有的教材普遍存在实用性不足的缺陷，导致高校和培训机构只能支付远超出预算的费用，或打破原定教学计划，选择《网管员必读》系列等实用性强的零售图书作为培训教材。正是充分体会到这些高校和培训机构的无奈，以及响应教师们一再提出希望我们能出一套适合教学和培训的网管类教材的要求，《网管第一课》系列图书应运而生。

本系列共 5 本图书，分别是：《网管第一课——计算机网络原理》、《网管第一课——网络组建与管理》、《网管第一课——网络应用与故障排除》、《网管第一课——网络操作系统与配置管理》和《网管第一课——计算机与网络安全》。

《网管第一课——计算机网络原理》：以 OSI 七层结构为主线，系统地介绍了各层主要的技术原理和应用，同时在本书的前两章从宏观角度分别介绍了计算机网络和计算机局域网。

《网管第一课——网络组建与管理》：按照一般的中小型网络组建思路，全面地介绍了中小型网络组建的各主要知识点，如拓扑结构设计与绘制、双绞线信息模块的制作、局域网设备互联与配置、家庭/宿舍网络方案与配置、中小型校园网络方案、中小型企业网络方案，在本书的最后还介绍了基本的网络管理知识和中小型网络中常用的网络管理工具。

《网管第一课——网络应用与故障排除》：本书较全面地介绍了当前在中小型企业网络中常见应用服务器的配置和故障排除方法，其中包括：IIS 6.0 Web 服务器、IIS 6.0/Serv-U FTP 服务器、POP3/CMail 邮件服务器，并在本书的第 1 章介绍了各种应用服务器共用的动态域名服务和端口映射配置。另外，在本书的后几章中还介绍了网络打印机的配置与维护、远程协助和远程管理的应用与故障排除，主要操作系统的应用故障排除，主要网络服务器的故障排除，以及网络设备的常见故障排除。

《网管第一课——网络操作系统与配置管理》：本书首先综合介绍了目前市场中主流的网络操作系统基础知识，然后以 Windows Server 2003 R2 版本为蓝本，系统地介绍了在中小型网络管理中需要用到的各种配置与管理方法，其中包括域控制器、DNS 服务器、DHCP 服务器的配置与管理，以及域用户和组管理、磁盘和文件管理、组策略管理和文件服务器管理。

《网管第一课——计算机与网络安全》：本书系统地介绍了与计算机和计算机网络有关的基础安全技术和应用，如密码技术、计算机病毒/木马/恶意软件的清除和预防、黑客攻击及其防御、防火墙技术和应用、入侵检测与入侵防御、文件加密与数字签名、主要操作系统的基础安全配置。

这5本书覆盖了一个网络管理员需要掌握的网络基础、网络组建、网络应用、网络管理、网络操作系统配置与管理、计算机和网络安全、常见网络故障排除等7个主要方面。本系列图书的主要特点就是在符合高校和培训机构教学特点和需求的前提下，采用全示例的讲解方式，突出强调高度的实用性和可操作性。学员通过对这5本书的连贯阅读和系统学习，可以实现由一个网络管理技术入门者向一名合格中小企业网管员的跨越。

《网管第一课》系列特色

本套图书的特色非常鲜明，主要体现在以下几个方面。

■ 定位于准网管和初级网管

区别于市面上常见的网管类图书，本系列图书充分体现了“第一课”这一主题和特色，紧紧围绕“网管入门”这一核心定位来安排和组织内容。常规网管类图书的目标读者范围较大，对准网管和初级网管这一群体的关注度和针对性不强。由于本系列图书具备“第一课”这一鲜明的定位，在具体内容与讲解形式上均有明显的倾向。本系列图书中所介绍的主要内容全部为网管员必须掌握的最基础、最重要的部分。

■ 示例化介绍

对于初级网管员，最需要的就是手把手式的示例介绍，而且此阶段需要掌握的理论知识并不多，不必进行深入的分析，只需要熟悉并掌握具体的操作步骤即可。本系列图书中，除了第一本《网管第一课——计算机网络原理》外，其他各本图书均是以示例为主线进行介绍的。读者通过对这些示例的学习，再结合《网管第一课——计算机网络原理》一书中的理论基础，就可以在自身实践中做到举一反三、融会贯通，根据实际情况灵活地为自己所在公司部署网络组建、应用、管理和安全维护方案。

■ 系统而全面

这是本系列图书最大的特点，也是目前读者最需要的。本系列图书尽管没有全面囊括网络管理知识的各个方面，但并未遗漏准网管和初级网管员必须掌握的所有主要知识点和技能，因此很好地保证了知识框架和学习要点的系统性和完整性。读者不必购买其他同类图书，就可以比较全面地学习到网管员所必须掌握的知识和技能。

■ 实用性强

这是许多图书争相标榜的优点，但实际上真正实用的图书并不多。虽然本系列图书的篇幅都不是很长，但可以说书中的每一部分内容都是经过认真甄选并提炼出来的相应知识领域的精华。为精简篇幅和提高阅读效率，本书未保留任何实用性较弱或学习紧迫性不强的章节，甚至段落，读者朋友可以在掌握一个个不可或缺的知识点的过程中，体会到学习的轻松与便捷。

期待着我们的努力能得到广大读者朋友、高等学校和培训机构的认可，期待着我国网管类教学和培训图书市场走向规范，走向高质量、高水平。当然，最期待的还是看了这一系列图书的读者朋友能有所收获，为日后正式成为一名合格的网管员甚至网络工程师，打下坚实的基础。衷心希望《网管第一课》能成为培育职业网管的摇篮！

飞思科技产品研发中心

王达

关于飞思

我们经常感谢生活的慷慨，让我们这些原本并不同源的人得以同本，为了同一个梦想走到一起。

因为身处科技教育前沿，我们深感任重道远；因为伴随知识更新节奏的加快，我们一刻也不敢停歇。虽然我们年轻，但我们拥有：

“严谨、高效、协作”的团队精神

全方位、立体化的服务意识

实力雄厚的作者群和开发队伍

当然，最重要的是我们还拥有：

恒久不变的理想

永不枯竭的激情和灵感

正因如此，我们敢于宣称：

飞思科技＝丰富的内容+完美的形式

这也是我们共同精心培育的品牌 

的承诺。

“问渠哪得清如许，为有源头活水来”。路再远，终需用脚去量；风景再美，终需自然抚育。

年轻的飞思人愿做清风细雨、阳光晨露，滋润您发芽、成长；更甘当坚实的铺路石，为您铺就成功之路。

FOREWORD

前　言

IT 安全已成为当前各行各业信息服务的一个热点，也是一个难点。无论是个人用户，还是企业网络用户，面对各种各样的 IT 安全技术，作为初涉网管行业的我们可能无所适从。这时，笔者认为最好的学习方法就是从自己的计算机，从自己所管理的小型局域网开始。本书正是基于这个考虑来策划并编写的，为各位提供 IT 安全领域的入门捷径。

本书的各章内容都是精心选择的，都是我们在安全管理入门时必须要了解或掌握的。全书共 8 章，第 1 章从宏观角度全面介绍了计算机和网络所面临的主要安全威胁和隐患，以及大家在企业网络安全认识上所存在的一些误区，使大家首先从宏观角度了解我们需要掌握的安全技术和 IT 安全管理方法。后面 7 章分别具体介绍了计算机和网络安全管理的一些主要方面，如计算机病毒、木马和恶意程序的预防与清除，个人计算机的安全设置、系统漏洞扫描与修复，黑客攻击和预防，网络防火墙及配置应用，IDS（入侵检测）和 IPS（入侵防御）及应用，文件加密与数字签名。其中，绝大多数都是当前网络安全技术和应用的热点，甚至是最新技术。

本书主要特点如下：

■　系统性强

虽然本书所介绍的安全知识不是很全面，也不是很深入，但对于刚接触 IT 安全的初级网管，甚至准网管来说，本书所介绍的章节已可以构成最基本的计算机和网络安全知识体系。其中就包括个人计算机系统的安全设置、计算机病毒、木马和恶意程序的预防和清除，漏洞扫描与修复、黑客攻击与预防、防火墙的配置与应用、IDS 与 IPS 技术和应用，以及文件加密与数字签名等。通过这几章的学习，可以达到快速登堂入室的效果。

■　重点突出

本书所介绍的知识点比较多，已构成了一个小的 IT 安全体系。同时本书所介绍的内容重点突出，使读者可以迅速地知道哪些是自己要重点掌握的。如本书的第 2 章、第 3 章、第 5 章、第 6 章和第 9 章是重点，介绍得比较全面、详细，所占用的篇幅也比较多。

■　实用性高

本书在技术理论上所占用的篇幅比较多，因为这是基础，不得不介绍。况且我们是初级网管，对基础的掌握更应当重视。同时，笔者在介绍书中的每一章时都结合了当前实际的计算机或企业网络安全管理需求，例举了大量的技术或产品应用示例，使得本书的实用性得到了充分保证。

本书由王达主笔并统稿，参加编写、校验和排版的人员有：何艳辉、王珂、沈芝兰、马平、何江林、刘凤竹、卢京华、周志雄、洪武、高平复、周建辉、孔平、尚宝宏、姚学军、刘学、李翔、王娇、李敏、吴鹏飞等。由于编者水平有限且时间仓促，尽管我们花了大量时间和精力校验，但书中可能还存在一些错误，敬请各位读者批评指正，万分感谢！

本系列丛书的 6 个读者专用 QQ 群为：17201450、21566766、32354930、5208368、13836245 和 4789821，专用博客和技术圈子分别为：http://winda.blog.51cto.com/ 和 http://group.51cto.com/lycb，欢迎加入其中讨论各种网络技术问题，交流工作经验和心得。也可以把您的问题发表在圈子中，我们会及时给予解答。

编 著 者

联系方式

咨询电话：（010）68134545　88254160

电子邮件：support@fecit.com.cn

服务网址：http://www.fecit.com.cn　http://www.fecit.net

通用网址：计算机图书、飞思、飞思教育、飞思科技、FECIT

CONTENTS

目　录

CHAPTER 1

第 1 章　计算机与网络安全概述

关键知识点或名词术语	对应章节
主要的计算机安全威胁	1.1.1
主要的网络安全威胁	1.1.2
企业网络的主要安全隐患	1.1.3
企业网络的十大安全认识误区	1.1.4
计算机病毒、计算机病毒的主要特点	1.2.3
计算机病毒的分类	1.3
木马、木马入侵行为的组成	1.4.1
木马与计算机病毒的区别	1.4.2
木马的伪装方式	1.4.3
木马的运行方式	1.4.4
恶意软件、恶意软件的主要特征	1.5.1
恶意软件的分类	1.5.2

内容提要	本章重点
本章介绍的是最基础的计算机和网络安全知识，其中包括计算机和网络的主要安全威胁、企业安全隐患和当前存在的安全认识误区，以及计算机病毒、木马和恶意软件的分类和各自的基本特征	■ 个人计算机存在的主要安全威胁 ■ 企业网络存在的主要安全威胁 ■ 企业网络的主要安全隐患 ■ 当前存在的企业网络认识误区 ■ 什么是计算机病毒、计算机病毒的分类，以及它们的主要危害 ■ 什么是木马，以及木马的主要特征及危害 ■ 什么是恶意软件、恶意软件的分类，以及各自的主要危害

1.1 计算机与网络安全概述

在IT领域说到安全，首先想到的是计算机系统本身的安全，因为它直接威胁到终端用户。计算机网络安全是随着计算机网络的普及而出现的一个新课题。现在讲安全，已不再像以前那样仅简单地谈计算机病毒，而是要面对各种除计算机病毒之外的木马、恶意软件和黑客入侵与攻击。安全的防御也不再是仅安装了防计算机病毒软件和防火墙就可以达到目的。现在的安全已自成体系，涉及OSI参考模型的各个层次。本节先来介绍一下计算机和计算机网络的安全威胁。

1.1.1 主要的计算机安全威胁

对于个人计算机来说，其安全性要求相对较低，因为通常不会成为黑客主动攻击的目标。就其安全威胁而言，主要存在以下几个方面。

1. 计算机病毒

无论是个人计算机，还是后面介绍的计算机网络，计算机病毒的威胁是最常见，也是最主要的。现在几乎每天都有大量新的计算机病毒产生，而且其危害性和破坏力一个比一个厉害。当然，计算机病毒也有好多种，具体将在本章后面进行介绍。

计算机病毒的危害主要体现在破坏计算机文件和数据，导致文件无法使用，系统无法启动；消耗计算机CPU、内存和磁盘资源，导致正常服务无法进行，经常死机、占用大量的磁盘空间；有的还会损坏计算机硬件，导致计算机彻底瘫痪。

针对计算机病毒的防护，首先是要安装个人或者网络版计算机病毒防护软件，让防病毒软件自动监测并查杀已感染的病毒，当然也可以进行一些手工清除，但相对来说比较困难。本书的第2章将介绍一些典型计算机病毒的手工清除与预防方法。

2. 木马

木马又称“后门程序”。虽然以前我们一直说木马不是病毒，不过现在仍有许多媒体把木马归属于病毒。但木马与病毒确实存在许多本质上的区别，具体也将在本章中详细介绍。

木马的主要危害体现在窃取用户信息（如用户计算机或网络账户和密码、银行账户和密码、QQ账户和密码等）；携带计算机病毒，造成计算机或网络运行不正常，甚至瘫痪；或者被黑客所利用，攻击用户计算机或网络。本章后面将具体介绍木马的分类和特色，有关木马的清除将在本书的第2章介绍。

3. 恶意软件

恶意软件是危害性介于计算机病毒与黑客软件之间的软件统称。恶意软件的危害性主要体现在非授权安装，自动拨号、自动弹出各种广告界面、恶意共享和浏览器劫持等。这些恶意软件一般都很难，甚至无法删除。具体特征将在本章后面介绍。而有关的恶意软件清除方法将在本书的第2章进行介绍。

1.1.2　主要的网络安全威胁

相对个人计算机而言，计算机网络的安全威胁除具有计算机安全中所介绍的 3 种常见威胁外，另一种就是黑客的入侵与攻击。

黑客入侵与攻击是指一类行为，不是指一类软件，更不是指一个软件。黑客入侵与攻击的目的主要是破坏网络用户系统或服务器系统，窃取用户账户信息和组织机密，并非法查看、操作，甚至删除用户文件等。

黑客入侵与攻击时所使用的软件非常多，可以是像我们正常网络检测或管理时所使用的工具软件，如 Ping、Telnet 等，还可以是一些控制能力非常强的专门工具，如流光（Fluxay）、灰鸽子（Huigezi）、网络间谍（NETSPY）等。现在借助于木马进行的攻击行为有所增加，用户一定要特别注意，如近期利用灰鸽子木马窃取用户银行账户的事件时有发生。

黑客攻击所带来的危害是最大的，它可以使整个网络处于瘫痪，也可以使我们的各种应用服务器崩溃，更可以轻松地窃取网络中的用户账户信息，特别是高权限的用户账户，从而达到为所欲为的目的。但要注意的是，这里所说的黑客入侵与攻击不仅是指来自外网用户的入侵与攻击，内部网络中同样可能存在这样的安全威胁，所以千万别只顾防外，而不防内。

对于黑客攻击行为最有效的手段就是采取主动预防策略，因为如果入侵与攻击行为一旦发生，所造成的损失可能是无法估量的。可以采取的方法非常多，如在防火墙、其他网络设备或软件工具（如路由器、本地或域安全策略、安全配置工具）中配置各种有效的安全策略，利用入侵检测和入侵防御工具主动发现并拦截攻击，利用网络隔离工具对关键用户或网络进行隔离等。本书在后面各章中将分别予以介绍。

1.1.3　企业网络的主要安全隐患

隐患不等于威胁，隐患来源于各种安全威胁。隐患所涉及的面要比威胁本身广很多，因为同一个威胁可能在不同方面造成安全隐患。

个人网络安全一般来说仅限于与因特网连接时的网络安全，它唯一的安全隐患来源就是因特网，但对于企业网络，其网络安全隐患不仅来自像因特网这样的外网，内部局域网的安全隐患也十分值得重视，而且外网中存在的安全隐患同样可以在内网中发生。也就是企业网络安全隐患有内、外网之分。正因为如此，企业网络安全策略的设计所考虑的就不仅仅是病毒入侵、外网攻击这么简单了。但要注意的是，在企业网络中，内、外网安全隐患又不是完全孤立的，在许多情况下，对外网安全威胁的最终来源是内网。

作为企业 IT 经理或网管员，要为自己的企业部署网络安全系统，首先要弄清楚的就是自己企业网络安全隐患。只有知己知彼，方能百战不殆。现在网络安全系统所要防范的不再仅是病毒感染，更多的是那些基于网络的非法入侵、攻击与访问。如果认识不足，很可能给企业网络留下许多的安全隐患。由于企业网络安全隐患的来源有内、外网之分，所以作为 IT 经理或企业网管员必须要全面地考虑问题，不要顾此失彼，千万别小看内部网络中存在的安全隐患。在很多情况下内部网络的安全威胁要远远大于外部网络，因为在内部网络中实施入侵和攻击更加容易。下面是一些主要的安全隐患。