ITAT

教育部实用型信息技术人才培养系列教材

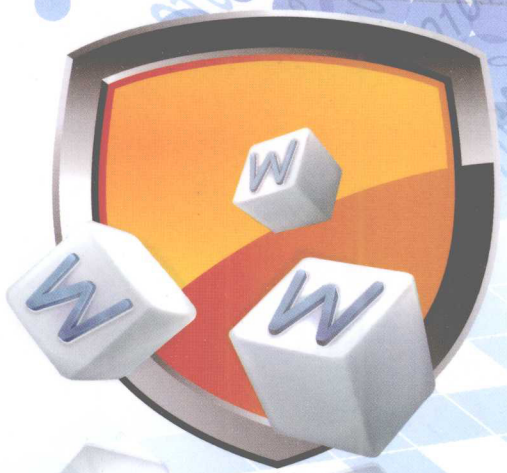
边用边学

电子教案

网络安全技术

杨永川 黄淑华 魏春光 编 著

全国信息技术应用培训教育工程工作组 审 定



机械工业出版社
CHINA MACHINE PRESS

教育部实用型信息技术人才培养系列教材

边用边学网络安全技术

杨永川　黄淑华　魏春光　编著
全国信息技术应用培训教育工程工作组　审定

机 械 工 业 出 版 社

本书是“教育部实用型信息技术人才培养系列教材”之一。本书针对计算机学科的特点，系统、全面地介绍了构建安全网络体系结构所需要掌握的理论和实践基础知识。书中没有过多地讲述原理，而是采用任务驱动的方式撰写，通过实例讲述导出概念、知识点和技术要点，将复杂的网络安全原理及应用技术以清晰和易于接受的方式介绍给读者。

本书共10章，主要包括网络安全的概念与性质、典型的网络威胁与攻击、数据加密技术及PKI、实体安全及访问控制、防火墙技术与配置、VPN技术与配置、入侵检测技术与产品、恶意代码分析及防范技术、Windows 2000操作系统安全加固，以及应用服务安全加固等内容。

本书结构清晰、合理，内容丰富、实用、新颖，适合普通高等院校、高等职业学校、高等专科学校、成人高等学校，以及各类计算机培训中心作为教学用书和培训教材，亦可作为读者在今后实践中有效的工具书和参考书。

图书在版编目(CIP)数据

边用边学网络安全技术/杨永川，黄淑华，魏春光编著. —北京：机械工业出版社，2009.10
(教育部实用型信息技术人才培养系列教材)
ISBN 978-7-111-28187-0

Ⅰ. 边… Ⅱ. ①杨… ②黄… ③魏… Ⅲ. 计算机网络-安全技术-教材 Ⅳ. TP393.08

中国版本图书馆CIP数据核字(2009)第153615号

机械工业出版社(北京市百万庄大街22号 邮政编码100037)
责任编辑：唐德凯
责任印制：李 妍
北京汇林印务有限公司印刷

2010年3月第1版·第1次印刷
184mm×260mm·19.75印张·487千字
0001-3000册
标准书号：ISBN 978-7-111-28187-0
定价：33.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务
社服务中心：(010)88361066
销 售 一 部：(010)68326294
销 售 二 部：(010)88379649
读者服务部：(010)68993821

网络服务
门户网：http://www.cmpbook.com
教材网：http://www.cmpedu.com

教育部实用型信息技术人才培养系列教材编辑委员会

（暨全国 ITAT 教育工程专家组）

出 版 说 明

信息化是当今世界经济和社会发展的大趋势，也是我国产业优化升级和实现工业化、现代化的关键环节。信息产业作为一个新兴的高科技产业，需要大量高素质复合型技术人才。目前，我国信息技术人才的数量和质量远远不能满足经济建设和信息产业发展的需要，人才的缺乏已经成为制约我国信息产业发展和国民经济建设的重要瓶颈。信息技术培训是解决这一问题的有效途径，如何利用现代化教育手段让更多的人接受到信息技术培训是摆在我们面前的一项重大课题。

教育部非常重视我国信息技术人才的培养工作，通过对现有教育体制和课程进行信息化改造、支持高校创办示范性软件学院、推广信息技术培训和认证考试等方式，促进信息技术人才的培养工作。经过多年的努力，培养了一批又一批合格的实用型信息技术人才。

全国信息技术应用培训教育工程（简称 ITAT 教育工程）是教育部于 2000 年 5 月启动的一项面向全社会进行实用型信息技术人才培养的教育工程。“ITAT”教育工程得到了教育部有关领导的肯定，也得到了社会各界人士的关心和支持。通过遍布全国各地的培训基地，ITAT 教育工程建立了覆盖全国的教育培训网络，对我国的信息技术人才培养事业，起到了极大的推动作用。

ITAT 教育工程被专家誉为“有教无类”的平民学校，以就业为导向，以大、中专院校学生为主要培训目标，也可以满足职业培训、社区教育的需要。培训课程能够满足广大公众对信息技术应用技能的需求，对普及信息技术应用起到了积极的作用。据不完全统计，在过去六年中共有五十余万人次参加了 ITAT 教育工程提供的各类信息技术培训，其中有近二十万人次获得了教育部教育管理信息中心颁发的认证证书。工程为普及信息技术、缓解信息化建设中面临的人才短缺问题做出了一定的贡献。

ITAT 教育工程聘请来自清华大学、北京大学、人民大学、中央美术学院、北京电影学院、中国传媒大学等单位的信息技术领域的专家组成专家组，规划教学大纲，制定实施方案，指导工程健康、快速地发展。ITAT 教育工程以实用型信息技术培训为主要内容，课程实用性强，覆盖面广，更新速度快。目前工程已开设培训课程二十余类，共计五十余门，并将根据信息技术的发展，继续开设新的课程。

本套系列教材由清华大学出版社、人民邮电出版社、机械工业出版社、北京希望电子出版社等出版发行。根据工程教材出版计划，全套教材共计六十余种，内容将汇集信息技术及应用各方面的知识。今后将根据信息技术的发展不断修改、完善、扩充，始终保持追踪信息技术发展的前沿。

全国 ITAT 教育工程的宗旨是：树立民族 IT 培训品牌，努力使之成为全国规模最大、系统性最强、质量最好，而且最经济实用的国家级信息技术培训工程，培养出千千万万个实用型信息技术人才，为实现我国信息产业的跨越式发展作出贡献。

全国 ITAT 教育工程负责人
系列教材执行主编　　薛玉梅

前　言

计算机网络安全是一个随着互联网的发展而不断引起人们关注的课题。发展迅速的互联网广泛应用于金融、电信、能源、交通运输、水供给、国土资源及社会保障等重要领域，成为国家的关键基础设施，同时深入到人们日常生活的各个方面。与此同时，有害信息、黑客入侵、病毒、木马也在网络空间中泛滥……安全问题愈演愈烈。人们已经清醒地认识到，在发展信息网络技术的同时，做好网络安全方面的理论研究与实践应用，是信息化的重要内容。

本书是“教育部实用型信息技术人才培养系列教材”之一。作者在整理、收集网络安全方面各种有关的资料，并结合自身的教学、科研和网络运行管理经验的基础上编写了本书。本书针对计算机学科的特点，系统、全面地介绍了构建安全的网络体系结构所需要掌握的理论和实践基础知识。书中没有过多地讲述原理，而是采用任务驱动方式撰写，通过实例讲述导出概念、知识点和技术要点，将复杂的网络安全原理及应用技术以清晰和易于接受的方式介绍给读者。

本书在内容上分为10章。

第1章网络安全概述，主要介绍了当前网络安全领域发展的现状，网络安全的内涵与外延，网络安全要解决的核心问题，以及网络安全的政策法规与标准。

第2章典型的安全威胁与攻击技术，主要分析了攻击者如何利用各种手段，通过本地或者网络，对目标进行攻击。

第3章密码技术及其应用，主要对构成网络安全基本防护技术的常见加密算法及其应用，如完整性校验、数字签名等进行了说明。

第4章实体安全与容灾备份，主要对计算机设备、设施（含网络）及其他媒体免遭地震、水灾、火灾、有害气体和其他环境事故（如电磁污染等）破坏的措施和过程进行阐述，并补充介绍了容灾系统的基本概念及关键技术。

第5章防火墙技术与配置，重点介绍了防火墙技术原理及其结构，并结合实例给出了防火墙的部署。

第6章VPN技术与配置，重点介绍了VPN技术原理及其应用，并结合实例给出了VPN的部署及配置。

第7章入侵检测技术与产品，重点分析了入侵检测技术原理及其结构，并结合实例给出了入侵检测系统的部署及配置。

第8章恶意代码分析与防御技术，首先介绍恶意代码的基本知识，包括定义、分类、起源与发展及其基本特征；然后按类别描述其重要的工作机理；最后总结恶意代码的一般防治方法，并给出网络环境下恶意代码的预警和防范体系。

第9章Windows 2000系统安全加固，重点介绍了增强Windows 2000系统安全性的配置方案。

第10章应用服务安全加固，主要对常用的互联网服务（如Web、FTP及电子邮件服务）的安全增强方案进行介绍。

本书在内容安排上循序渐进，由浅入深地剖析了网络安全面临的威胁和典型攻击实例，并有针对性地给出了防范技术和配置、实施方法。书中给出的范例具有可操作性，读者完全可以参照实例的策略和配置，结合详细的操作步骤和方法，来掌握网络安全的相关基础知识。

本书由全国信息技术应用培训教育工程工作组组编，薛佳和王彦峰对本书进行了审定。在本书的编写和出版过程中，得到了教育部教育管理信息中心、中国人民公安大学信息安全工程系、中国人民公安大学网络中心的大力支持和帮助，在此，向上述单位的有关领导和同志，以及本书引用的有关文献的编著者，表示衷心的感谢。

由于作者水平有限，书中难免存在疏漏和欠妥之处，敬请读者批评指正。

作　者

目　录

第1章　网络安全概述

1969年，互联网的雏形诞生了：连通犹他大学、斯坦福大学、加州大学洛杉矶分校和加州大学巴巴拉分校4个节点的分组交换实验网络互联成功。1972年，第一个互联网络ARPANet投入使用。之后，互联网发展迅速，广泛应用于金融、电信、能源、交通运输、水供给、国土资源及社会保障等重要领域，成为国家的关键基础设施，同时深入到人们日常生活的各个方面。然而，伴随着网络的普及，几乎每天都有非法闯入和安全侵犯事件的新闻：有害信息污染严重，黑客入侵和网络攻击频繁发生，计算机病毒蔓延和泛滥，机要信息流失和信息间谍潜入，涉及网络的计算机犯罪案件以指数增加，信息战的阴影也不可忽视……安全问题越来越引起人们的关注。

1.1　网络安全问题溯源

学习目标：

- 了解网络存在安全威胁的根本原因。
- 明确系统脆弱性。
- 理解网络协议和服务的脆弱性。

由于技术发展、工艺水平及设计者的经验等各种条件的限制，网络系统各个部分的设计本身有可能存在导致安全隐患的漏洞。网络中的硬件、软件、系统配置及各种网络协议的设计，其中任何一部分在安全方面的瑕疵都可能造成网络的安全脆弱性。

1.1.1　系统的脆弱性

1. 硬件系统的脆弱性

计算机硬件系统的脆弱性主要来自于以下方面。

1）计算机信息系统的硬件均需要提供满足要求的电源才能正常工作，一旦切断电源，哪怕是极其短暂的一刻，计算机信息系统的工作也会被间断。

2）计算机是利用电信号对数据进行运算和处理的。因此，环境中的电磁干扰能引起处理错误，得出错误的结论，并且所产生的电磁辐射会产生信息泄露。

3）电路板焊点过分密集，极易产生短路而烧毁器件。接插部件多，接触不良的故障时有发生。

4）体积小、重量轻、物理强度差，极易被偷盗或毁坏。

5）电路高度复杂，设计缺陷在所难免，加上有些不怀好意的制造商还故意留有“后门”。

2. 操作系统的脆弱性

任何应用软件均是在操作系统的支持下执行的，操作系统的不安全是计算机信息系统不安全的重要原因。操作系统的脆弱性如图1-1所示。

操作系统的脆弱性表现在以下几个方面。

1）操作系统的程序可以动态链接。这种方式虽然为软件开发商进行版本升级提供了方便，但“黑客”也可以利用此法攻击系统或链接计算机病毒程序。

2）操作系统支持网上远程加载程序，这为实施远程攻击提供了技术支持。

3）操作系统通常提供 DEMO 软件。这种软件在 UNIX 和 Windows NT 操作系统上与其他系统核心软件具有同等的权利。借此摧毁操作系统十分便捷。

4）系统提供了 Debug 与 Wizard。它们可以将执行程序进行反汇编，方便追踪执行过程。

5）操作系统的设计缺陷。计算机病毒和“黑客”程序正是利用这些缺陷对操作系统进行致命攻击。

Number of OS Vulnerabilities by Year

OS	1997	1998	1999	2000
AIX	20	38	10	6
BSD (aggr.)	8	8	25	26
BSD/OS	6	5	4	0
BeOS	0	0	0	5
Caldera	2	2	13	11
Connectiva	0	0	0	11
Debian	2	2	30	20
FreeBSD	4	2	17	19
HP-UX	8	5	8	12
IRIX	28	13	9	12
Linux (aggr.)	11	23	92	82
MacOS	0	1	5	0
MacOS X Server	0	0	1	0
Mandrake	0	0	1	22
NetBSD	1	4	10	14
Netware	0	0	4	3
OpenBSD	1	2	4	7
RedHat	5	10	41	40
SCO Unix	1	3	9	2
Slackware	4	8	10	5
Solaris	24	31	34	9
SuSE	0	0	22	15

www.securityfocus.com

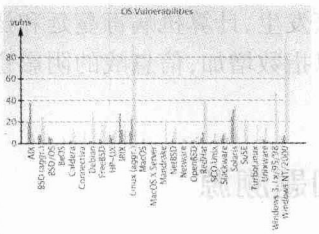


图 1-1　操作系统脆弱性

3. 存储系统的脆弱性

计算机的存储系统分为内存和外存：内存分为 RAM 和 ROM；外存有硬盘、软盘、磁带和光盘等。它们的脆弱性表现在如下几个方面。

1）RAM 中存放的信息一旦掉电即刻丢失，并且易于在内嵌入病毒代码。

2）硬盘构成复杂，既有动力装置，也有电子电路及磁介质，任何一部分出现故障均会导致硬盘不能使用，丢失其中的大量软件和数据。

3）软盘及磁带易损坏。它们的长期保存对环境要求高，保存不妥，便会发生霉变现象，导致数据不能读出。此外，盘片极易遭到物理损伤（折叠、划痕、破碎等），从而丢失其中的程序和数据。

4）光盘盘片没有附在一起的保护封套，在进行数据读取和存放的过程中容易因摩擦而产生划痕，引起读取数据失败。此外，盘片在物理上脆性较大，易破碎而损坏，导致磁盘上的数据丢失。

5）各种信息存储媒体的存储密度高，体积小，且重量轻，一旦被盗窃或损坏，损失巨大。

6）存储在各媒体中的数据均具有可访问性，数据信息很容易地被复制而不留任何痕迹。一台远程终端上的用户，可以通过计算机网络连接到你的计算机上，利用一些技术手段，访问到你系统中的所有数据，并按其目的进行复制、删除和破坏。

4. 传输系统的脆弱性

组建计算机网络的出发点是资源共享和数据通信。计算机之间需要借助交换设备和有线