计算机网络攻击与防范

冯前进 李龙景 主编

司法警官职业教育系列教材

中国政法大学出版社

司法警官职业教育系列教材

计算机网络攻击与防范

主编　冯前进　李龙景

中国政法大学出版社

图书在版编目（CIP）数据

计算机网络攻击与防范 / 冯前进，李龙景主编. —北京：中国政法大学出版社，2008.6
ISBN 978-7-5620-3237-3
Ⅰ.计... Ⅱ.①冯...②李... Ⅲ.计算机网络-安全技术 Ⅳ.TP393.08
中国版本图书馆CIP数据核字(2008)第084768号

出版发行 中国政法大学出版社
经　　销 全国各地新华书店
承　　印 固安华明印刷厂

787×960　16开本　22印张　415千字
2008年6月第1版　2008年6月第1次印刷
ISBN 978-7-5620-3237-3/D•3197
定　价：34.00元

社　　址 北京市海淀区西土城路25号
电　　话 (010)58908325（发行部） 58908285(总编室） 58908334(邮购部)
通信地址 北京100088信箱8034分箱　邮政编码 100088
电子信箱 zf5620@263.net
网　　址 http://www.cuplpress.com （网络实名：中国政法大学出版社）

司法警官职业教育系列教材
编 审 委 员 会

内容提要

本书是一本从实战出发，以应用为目的，以防范手段为重点，集理论性、实战性、应用性、操作性为一体，紧密跟踪计算机网络安全领域的热点问题、难点问题和最新防范技术运用的教材。教材从应用的角度，系统介绍了计算机网络攻击与防范所涉及的基础理论、攻击手段和防范技术。以阶段能力培养为目的，每个能力阶段为一个章节，每章内容开始有“教学提示”和“教学要求”，结束有“本章小结”、“习题”，部分章节还设计了实训内容。通过理论学习、实战演练，读者能够综合运用书中所讲授的技术进行网络攻击与防范方面的实践。

本教材注重实践技能的培养，以实训为依托，深入浅出地讲解理论知识，因此既可作为高职高专院校计算机及相关专业的学生教材，也可作为计算机网络安全类技术参考书或培训教材。

编写说明

为了适应司法警官高等应用性专门人才培养的客观需要，适应司法警官高等教育改革和发展的要求，在中国政法大学出版社的大力支持下，浙江警官职业学院组织编写出版了一套司法警官职业教育系列教材。

本套教材分为刑事执行、行政执行、司法警务、安全防范、法律事务、警务基础等六大类。教材编写根据司法警官高等职业院校人才培养目标和教育部对高职院校“突出实践应用能力培养、理论知识以必需够用为度”的教学要求，着重解决司法警官院校特有专业教材缺少的问题，同时积极进行精品（重点）课程教材建设，努力培育特色教材。在教材内容上，力求体现：

1. 时代性。本套教材以最新法律法规的规定为依据，努力吸收当前国内相关的最新学术理论研究成果，注意借鉴国外有关的研究成果，结合社会和行业实际发展，具有较强的时代性。

2. 实用性。本套教材在编写过程中贯彻实用性原则，坚持理论联系实际，采取理论研究与行业实际及实例说明相结合的形式，强调尽量满足学以致用和职业技能训练要求。在实例的选用上，均注重选用相关行业的实际案例，并经分析、整合、提炼后体现在文本中，以便学习者更易于接受。

3. 系统性。本套教材充分考虑到学科知识体系的相对完整性，注重对相应学科中的基本概念、基本原理和基本实务问题的分析和阐述，力求释义准确，论点明确，重点突出，结构严谨，逻辑严密，便于学

生系统地学习和掌握相关知识点。

4. 通俗性。教材作者立足警官院校的实际，针对高职学生的特点，力求运用通俗易懂、简明流畅的言语或简单的案例来阐释理论，尽量做到可读、易懂。

本套教材适用于全日制警官高等职业院校相关专业，也可供其他院校及相关行业从业人员作为教学、业务培训、自学用书。

本套系列教材（第一期）将在2005～2007年间陆续与大家见面。由于教材编写是一项复杂的系统工程，任务繁重，时间紧迫，因此不足之处在所难免，我们真诚地希望得到广大师生、读者的厚爱、谅解、批评和指正，以使本套教材不断修改、充实和完善，更好地为警官高等教育事业服务。

司法警官职业教育系列教材编审委员会

前　言

随着计算机网络技术的迅速发展，网络在经济、军事、文教、金融、商业等诸多领域得到广泛应用，可以说网络无处不在，它正在改变我们的工作方式和生活方式。计算机网络在给人们提供便利、带来效益的同时，也使人类面临着信息安全的巨大挑战。如何保护个人、企业、国家的机密信息不受黑客和间谍的入侵，如何保证计算机网络安全并不间断地工作，是国家和单位信息化建设必须考虑的重要问题。然而，计算机网络的安全是一个错综复杂的问题，涉及面非常广，既有技术因素，又有管理因素；既有自然因素，又有人为因素；既有外部的安全威胁，又有内部的安全隐患。

本教材作为计算机网络安全的专门教材，结合高职高专学生的实际情况，着重从实践角度讲解了网络安全概念、网络安全威胁、常见网络攻击手段、网络安全标准、网络安全防范策略及最新的网络安全防范技术。全书共分13章：第1章为计算机网络安全概述，对网络安全所涉及的相关问题进行了概要性描述；第2章主要介绍了计算机病毒与防治；第3章介绍了Windows 2000系统的安全防范；第4章介绍了Web应用服务安全防护手段；第5章介绍了数据库安全防范措施；第6章介绍了常见网络攻击的手段与防范方法；第7章～第11章分别介绍了“信息加密与PKI”、“访问控制技术”、“防火墙技术”、“入侵检测技术”、“VPN技术”等网络安全防范技术；第12章重点介绍了作为保证数据有效性、提高系统可靠性的重要手段——各份技术与灾难恢复策略；第13章主要介绍了无线网络的安全问题与防护技术，使

读者对“无线网络安全”这一前瞻性问题有一定的初步了解。

本书各章都配有习题，大部分章节配有相应的实训，以便于教学和自学。

通过对本教材的学习，读者可以系统了解常见计算机网络攻击手段，掌握计算机网络攻击与防范的基础知识和最新网络安全防范技术的应用技能。

本书由浙江警官职业学院冯前进、李龙景任主编，傅望、赵杰、陈佳莹任副主编并参与编写事宜。冯前进编写了第1、2、11、12章，李龙景编写了第7、13章，傅望编写了第8、9、10章，赵杰编写了第5、6章，陈佳莹编写了第3、4章。本书由冯前进副教授负责策划、统稿，李龙景教授审定。

在本书的编写过程中，我们得到了中国政法大学出版社的鼎力相助，并参考选用了相关资料，在此谨表谢意。

由于编者水平有限，时间仓促，欠缺之处在所难免，恳请广大读者批评指正。

冯前进　李龙景

2008年5月于杭州

目　录

第1章　计算机网络安全概述

✣教学提示

随着计算机网络技术的迅速发展，计算机网络的应用领域已从传统的数学运算、文件处理、基于简单连接内部网络的业务处理、办公自动化等小型业务系统，逐渐向大型关键业务系统扩展。随着政府上网、企业上网、教育上网、家庭上网等，互联网在经济、军事、文教、金融、商业等诸多领域得到广泛应用，可以说网络无处不在，它正在改变我们的工作方式和生活方式。计算机网络在给人们提供便利、带来效益的同时，也使信息安全面临着前所未有的巨大挑战，这就是网络安全问题。通过对本章的学习，希望大家能从宏观上对网络安全问题有比较全面的了解和把握。

✣教学要求

本章主要学习网络安全概念、网络安全威胁、常见网络攻击手段、网络安全标准、网络安全防范策略。

1.1　网络安全概念

以 Internet 为代表的全球性信息化浪潮所带来的影响日益深刻，信息网络技术的应用正日益普及，应用层次正在深入，应用领域从传统的小型业务系统逐渐向大型的关键业务系统扩展，典型的如党政部门信息系统、金融业务系统、企业商务系统等。伴随网络的普及，安全日益成为影响网络效能的重要因素，而 Internet 所具有的开放性、国际性和自由性在增加应用自由度的同时，对安全提出了更高的要求，这主要表现在以下两个方面：

（1）开放性的网络导致网络的技术是全开放的，任何组织和个人都可能获得，因而网络所面临的破坏和攻击可能是多方面的。例如：任何具有不良企图的黑客可以对物理传输线路实施攻击，也可以对网络通信协议实施攻击；可以对软件实施攻击，也可以对硬件实施攻击。网络的国际化还意味着网络的攻击不仅仅来自本地网络用户，可以来自 Internet 上的任何一台主机。也就是说，网络安全

面临的是一个国际化的挑战。

（2）自由意味着网络最初对用户的使用并没有提供任何的技术约束，用户可以自由地访问网络，自由地使用和发布各种类型的信息。用户只对自己的行为负责，而不受任何的法律限制。

开放的、自由的、国际化的 Internet 发展给政府机构、企事业单位带来了革命性的变革，使得人们能够利用 Internet 提高办事效率和增强市场反应能力，以便更具竞争力；同时人们又要面对网络开放所带来的数据安全的新挑战和新危险，如何保护内部机密信息不受黑客和工业间谍的入侵，已成为政府机构、企事业单位信息化建设所必须考虑的重要议题之一。

1.1.1 网络安全的概念

网络安全包括 5 个要素：机密性、完整性、可用性、可控性和不可否认性。机密性指确保信息不暴露给未授权的实体或进程；完整性则意味着只有得到授权的实体才能修改数据，并且能够判别出数据是否已被篡改；可用性是信息资源服务功能和性能可靠性的度量，是对信息网络总体可靠性的要求，即得到授权的实体在需要时可访问数据，攻击者不能占用所有的资源而阻碍授权者的工作；可控性主要指对危害国家信息的监视审计，控制授权范围内的信息流向及行为方式，使用授权机制，控制信息传播的范围、内容，必要时能恢复密钥，实现对网络资源及信息的可控性；不可否认性是对出现的网络安全问题提供调查的依据和手段，使用审计、监控、防抵赖等安全机制，使得攻击者、破坏者、抵赖者“逃不脱”、“赖不掉”，并进一步对网络出现的安全问题提供调查依据和手段，实现信息安全的可审查性，一般通过数字签名等技术实现不可否认性。

网络安全的定义从狭义的保护角度来看，是指计算机及其网络系统资源和信息资源不受自然和人为有害因素的威胁和危害；从广义来说，凡是涉及计算机网络上信息的机密性、完整性、可用性、可控性、不可否认性的相关技术和理论都是计算机网络安全的研究领域。

1.1.2 网络安全的现状

1.1.2.1 美国、西欧国家网络安全的现状

现在全球普遍存对网络安全重视不够的状况。人们在组建一个网络的时候，并没有意识到网络安全的重要性。这导致大多数网络存在着先天性的安全漏洞和安全威胁。

此外，从网络安全管理的角度来看，国际上也存在着信息安全管理规范和标

准不统一的问题。美国是西方国家中对信息安全着力较多的国家之一，同样存在着规范和标准跟不上技术进步发展的问题。西欧国家则另有一套信息安全标准，虽然在原理和结构上同美国有相同的部分，但是不同的部分也相当多。美国、西欧国家频频遭受黑客攻击，蒙受巨大经济损失，国家网络安全现状不容乐观。黑客攻击、计算机病毒破坏和网络金融犯罪已构成对世界各国的实际威胁。下面列举一些近年来发生的典型网络安全事件：

（1）1983 年，美国联邦调查局首次逮捕了 6 名少年黑客，因他们所居住地区密尔沃基的电话区号是 414，而被人称做“414 黑客”。这 6 名少年黑客被控侵入 60 多台电脑，其中包括斯洛恩 - 凯特林癌症纪念中心和洛斯阿拉莫斯国家实验室。

（2）1987 年，17 岁的高中学生赫尔伯特·齐恩（被执法当局称作“影子鹰”）承认侵入美国电话电报公司位于新泽西州贝特敏斯特市的电脑网络。美国联邦执法部门指控他（在芝加哥郊区的卧室里操纵一台电脑）闯入美国电话电报公司的内部网络和中心交换系统。齐恩是美国 1986 年“计算机欺诈与滥用法案”生效后被判有罪的第一位黑客。

（3）1988 年，美国康奈尔大学研究生罗伯特·莫里斯（22 岁）向互联网上传了一个“蠕虫”程序。这个程序是他为攻击 Unix 系统的缺陷而设计的，能够进入网络中的其它电脑并自我繁衍。当时使得美国 6000 多个系统（几乎占当时互联网的 1/10）陷入瘫痪。专家称他设计的“蠕虫”程序造成了 1500 万到 1 亿美元的经济损失。

（4）1990 年，“末日军团”（美国南方的一个黑客组织）的 4 名成员盗窃南方贝尔公司的 911 紧急电话网络的技术机密，4 名黑客中有 3 人被判有罪。

（5）1995 年，米特尼克被逮捕。他被指控闯入许多电脑网络，偷窃了 2 万个信用卡号和复制软件。他曾闯入“北美空中防务指挥系统”；破译了美国著名的“太平洋电话公司”在南加利福尼亚州通信网络的“改户密码”；入侵过美国 DEC 等 5 家大公司的网络。据专家们测算，米特尼克一人就造成了美国一些公司 8000 万美元的巨额损失。

（6）1998 年，美国国防部宣布黑客向五角大楼网站发动了“有史以来最大规模、最系统性的攻击行动”。黑客打入了许多政府非保密性的敏感电脑网络，查询并修改了工资报表和人员数据。3 个星期后，美国警方宣布以色列少年黑客“分析家”被抓获。

（7）2000 年 2 月，以“雅虎”为首的美国一系列大型网站遭到了黑客的有组织攻击，他们攻击的目标包括雅虎、电子港湾、亚马逊、微软网络等美国大型网站。据统计，在 2 月 7 日、8 日、9 日这短短的 3 天里，这些受害公司的损失

就超过了10亿美元，其中仅营销和广告收入一项就高达1亿美元。

（8）2000年5月4日开始发作的“I Love You”电脑病毒如野火一般肆虐美国公司，进而波及全球，使许多公司的生产大受影响。全球已造成100亿美元损失。

（9）2005年6月19日，据美国媒体报道：“全球最大的VISA卡服务商存储到计算机数据库中的4000万用户信息被人盗取。包括Visa（维萨）、MasterCard（万事达）、American Express（美国运通）和Discover（发现）在内的几家大信用卡公司4000万用户信息被盗，其中还殃及到中国内地持卡人持有的近9000张信用卡。”

（10）根据英国著名的DTI和PWC公司的调查显示，2003年英国有3/4的公司被网络黑客成功的突破了信息安全系统，这些公司因此所花费的资金高达数十亿英镑；有94%的公司发生过网络安全事故，而这一数字在2002年和2000年才分别是44%和24%；大型英国公司遭黑客袭击的比率是74%，平均每月一次，某些超大型公司甚至是每周一次，而每一次的网络安全事故所引起的相关费用就高达12万英镑。

1.1.2.2 国内网络安全的现状

我国的信息安全形势也不容乐观。我国自2000年以来，建设了一批信息安全基础设施，加强了互联网信息内容的安全管理，信息安全保障工作取得一些成效。但是由于基础薄弱，工作人员防范意识淡薄，安全隐患巨大。

（1）网上的重大失窃密案件多有发生。反动邪教法轮功和民运分子等境内外敌对势力利用因特网从事各种违法犯罪活动，对社会稳定和政权稳固造成了许多负面影响。

（2）计算机犯罪率逐年上升，我们国家计算机犯罪增长速度已经超过了传统犯罪的增长速度。根据公安部统计，1988年至1989年，仅发生计算机犯罪案件9起，1989年至1990年发生计算机犯罪案件上百起，1993年发生计算机犯罪案件1000多起，1994年为1450起，2000年公安机关立案侦查的计算机违法犯罪案件达到2700余起，2002年又涨到4500余起，比上年上升了70%。计算机犯罪的发案率成直线上升趋势。特别是我国网络金融安全隐患巨大，我国银行网络每年因安全问题包括外部攻击、内外勾结、内部人员违法犯罪和技术缺陷引起的经济损失数以亿计。

1986年7月，中国银行深圳市蛇口支行电脑主管陈新义伙同苏庆忠通过计算机骗取银行巨款，共计人民币2万余元，港币3万元，成为中国大陆第一例计算机犯罪案件；1994年4月，深圳市国际证券投资基金电脑部副经理罗世平利