网络安全专家

企业网络安全致胜宝典

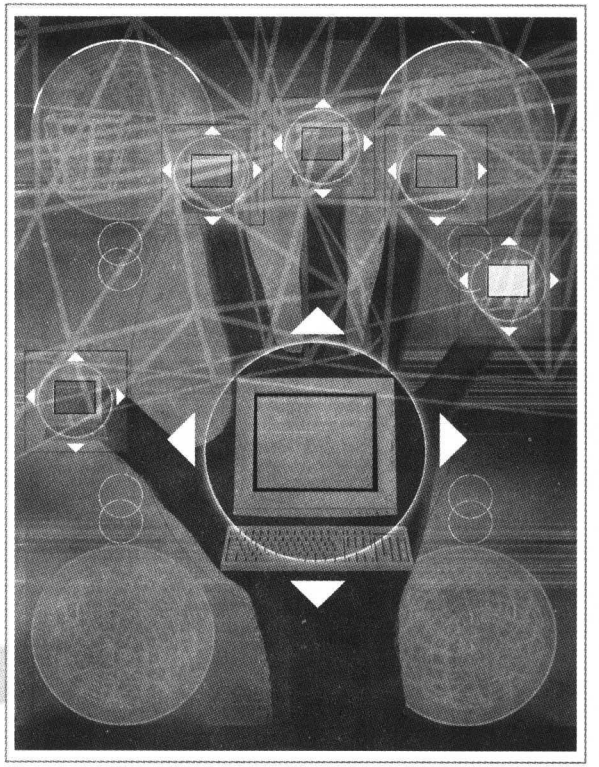
- 增强企业网络病毒的免疫力
- 特络伊木马揭秘
- 操作系统漏洞及攻防方法
- 企业服务器安全配置
- 从企业网站堵住大漏洞
- 安全网络所需的安全产品
- 安全风险管理ABC
- 企业入侵应急响应案例

郭鑫　崔红霞　姜彬　编著
飞思科技产品研发中心　监制

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

网络安全专家

企业网络安全致胜宝典



郭鑫　崔红霞　姜彬　编著
飞思科技产品研发中心　监制

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

内容简介

本书从介绍信息安全基本概念开始，介绍信息安全建设可以依据的各类体系结构，堪称网络安全致胜宝典。书中详细地讲解企业网络的个人计算机安全、企业服务器安全、网站程序安全、增强企业网络病毒的免疫力、木马如何控制企业网络、黑客入侵网络方式、网络安全产品、安全风险管理、企业应急响应案例等，最后得出结论：构筑企业网络安全体系，应该融合技术和管理的内容，并充分考虑到人、流程和工具这 3 个因素综合作用所构建的体系结构。

书中对网络管理员比较关心的大型网络入侵响应、犯罪取证和入侵事件的调查过程，做了全面的流程分析和操作，以使网络管理员改掉不良习惯，把网络安全风险降到最低限度。通过阅读本书，网络管理员及相关读者，一定能够更加有效地对网络进行安全加固和维护。

本书适合网络管理员、系统管理员阅读，对网络爱好者、网络使用者也有较高的参考价值。

图书在版编目（CIP）数据

企业网络安全致胜宝典 / 郭鑫，崔红霞，姜彬编著. —北京：电子工业出版社，2007.10
（网络安全专家）
ISBN 978-7-121-05095-4

Ⅰ. 企… Ⅱ.①郭…②崔…③姜… Ⅲ.企业－计算机网络－安全技术 Ⅳ.TP393.180.8

中国版本图书馆 CIP 数据核字（2007）第 147789 号

责任编辑：李泽才
印　　刷：北京机工印刷厂
装　　订：三河市鹏成印业有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编：100036
开　　本：787×980　1/16　印张：20.5　字数：393.6 千字
印　　次：2007 年 10 月第 1 次印刷
印　　数：6 000 册　定价：39.80 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。

反侵权盗版声明

出版说明

危机无处不在，防范刻不容缓。
无论身处网络技术链条的哪一个环节，
安全均不容忽视，且重要性日益突显。
——“网络安全专家”为你提供安全技术的知识结晶

网络安全技术发展迅速

随着 IT 应用的日益普及，计算机网络技术广泛应用于各行各业，形成各自的网络，为资源共享、信息交换和分布处理提供了广阔而又良好的环境。计算机网络具备分布广域性、结构开放性、资源共享性和信道共用性的特点。因此，在增加网络实用性的同时，不可避免地带来了系统的脆弱性，使其面临着严重的安全问题。现在，随着计算机网络资源共享的进一步加强，随之而来的网络安全问题日益突出，人们对计算机信息安全的要求也越来越高。计算机网络技术的普及和随之而来的网络安全问题，使得计算机网络安全保护变得越来越重要。黑客的攻击技术、网络通信安全技术策略和管理机制等，直接影响到网络安全，已被越来越多的网络用户所关注。

切中网络安全技术教育脉搏

鉴于网络信息安全对企业和个人用户的重要性，我们对信息安全类图书也做了比较完整的规划，特意为以下三类读者量身订制了“网络安全专家”系列丛书，希望可以为网络安全技术教育略尽绵薄。

◇ **面向最广大的安全技术人员（Operator）。**向网络信息安全领域的操作者/使用者/管理员，全面介绍企业、家庭信息安全领域的技术热点、解决方案，为该类读者提供强大而有效的技术支持。

◇ **面向企业安全管理人士（Manager）。**为项目主管/安全工程师/安全咨询师/IT 经理级人士，提供信息安全网络设计、管理、部署，以及企业安全评估、维护等项目管理类指导。

◇ **面向安全产品的开发者（Developer）。**针对开发人员热切关注的病毒研究、数据加密、攻击跟踪、检测反馈等相关知识，提供来自全球领先市场的先进思想、经验和技能。

“网络安全专家”丛书，已出版图书包括：《数据库加密——最后的防线》、《没有任何漏洞——信息安全实施指南》、《防黑档案》、《防黑档案（第 2 版）——黑客新招曝光》、《中国电脑救援中心网经典救援案例精粹》、《网络服务器安全配置详解》等，内容覆盖网络安全防范、网络安全工具、网络服务器、网络组建等各方面。

本丛书主要关注的技术和应用热点见下表。

黑客攻击手段	黑客攻击步骤	安全技术策略	访问控制策略
密码猜测	身份和位置	物理安全策略	入网访问控制
窥探	目标系统信息收集	加密技术	网络权限控制
电子欺骗	弱点信息挖掘分析	防火墙技术	目录级安全控制
信息剽窃	目标使用权限获取	入侵检测技术	属性安全控制
让主机拒绝服务	攻击活动隐蔽	反病毒技术	网络服务器安全控制
信息破坏	攻击活动实施	访问控制策略	……
……	开辟后门	身份认证技术	
	攻击痕迹清除	……	

“网络安全专家”五大看点

魔高一尺，道高一丈。网络安全是一个长期问题。世界上不存在绝对安全网络系统。虽然市面上网络安全类图书层出不穷，但随着计算机硬件、软件的不断更新换代，系统越来越复杂，对网络安全技术要求也越来越高，读者需求也随之不断变化。因此，只有不断跟踪与捕捉广大网络用户普遍关心的技术与应用的热点，才能将真正实用、有效的知识和技能，及时地呈现在读者面前。

◇ 推荐看点之一：权威观点，专家视角

与国外 Symantec Press 等长期专注于信息安全领域的专业出版社合作，使国内读者共同分享全球顶级安全专家的精华思想与宝贵经验。

◇ 推荐看点之二：关注行业，重视实践

以网络安全行业发展趋势为指导，以前沿技术与应用实践为核心，为行业上下游人群提供技术领先且行之有效的实战技能。

◇ 推荐看点之三：项目管理，机制在先

安全管理是网络安全的关键环节，而先进的项目管理思想、稳定的系统运行机制，以及高效的信息化手段正是国内所缺，我们将重点关注，全力打造相关精品。

◇ 推荐看点之四：聚焦行业，助力成才

网络安全行业的从业者是维护网络安全的中坚力量。本丛书将竭诚为其提供职业上的指导与帮助，围绕其所需所想，有针对性地创新产品。

◇ 推荐看点之五：贴近读者，易读为要

网络安全防护是一门综合学科，需要深入而系统地掌握相关理论知识。因此，易懂、易学和易用，将是我们为普及网络安全技术做出的重要承诺。

我们相信，在广大读者、作者的不断关注下，我们的承诺一定会稳步实现！

飞思科技产品研发中心

前　言

随着信息化进程的深入和互联网的迅速发展，人们的信息资源得到最大程度的共享。但必须看到，紧随信息化发展而来的网络安全问题日渐突出，如果不很好地解决这个问题，必将阻碍信息化发展的进程。

在各领域的计算机犯罪和网络侵权方面，无论是数量、手段，还是性质、规模，已经到了令人咋舌的地步。据有关方面统计，目前美国每年由于网络安全问题而遭受的经济损失已超过 170 亿美元，德国、英国也均在数十亿美元以上，法国为 100 亿法郎，日本、新加坡问题也很严重。在国际刑法界列举的现代社会新兴犯罪排行榜上，计算机犯罪已名列榜首。2003 年，CSI/FBI 调查所接触的 524 个组织中，有 56%遇到电脑安全事件，其中 38%遇到 1～5 起、16%遇到 11 起以上。因与互联网连接而成为频繁攻击点的组织连续 3 年不断增加。遭受拒绝服务攻击从 2000 年的 27%上升到 2003 年的 42%。调查显示，521 个接受调查的组织中 96%有网站，其中 30%提供电子商务服务，这些网站在 2003 年 1 年中有 20%发现未经许可入侵或误用网站现象。更令人不安的是，有 33%的组织说他们不知道自己的网站是否受到损害。据统计，全球平均每 20 秒就发生 1 次网上入侵事件。

电脑黑客活动已形成重要威胁。网络信息系统具有致命的脆弱性、易受攻击性和开放性。从国内情况来看，目前我国 95%与互联网相连的网络管理中心，都遭受过境内外黑客的攻击或侵入，其中银行、金融和证券机构是黑客攻击的重点。

信息基础设施面临网络安全的挑战。面对信息安全的严峻形势，我国的网络安全系统在预测、反应、防范和恢复能力方面存在着许多薄弱环节。据英国《简氏战略报告》和其他网络组织对各国信息防护能力的评估，我国被列入防护能力最低的国家之一，不仅大大低于美国、俄罗斯和以色列等信息安全强国，而且排在印度、韩国之后。近年来，国内与网络有关的各类违法行为以每年 30%的速度递增。

就像建造一座大厦需要事先设计蓝图一样，进行信息安全建设，也需要有一个实施依据，即从整体上考虑的信息安全体系。信息安全要做成什么“模样”？信息安全建设应该考虑到哪些方面？到底什么才是全面而完整的信息安全？这些问题都需要通过安全体系的设计来回答。只有在整体的安全体系指导下，信息安全建设所需的技术、产品、人员和操作等，才能真正发挥各自的效力。作为信息

安全建设的指导方针，安全体系的设计应该体现出可靠性、完备性、可行性和可扩展性原则。企业安全体系构建要依据有效蓝图来进行。蓝图要求具有完整、可实施和可操作。这就是个体系的问题了。本书从信息安全基本概念切入，介绍信息安全建设依据的各类体系结构，最终得出结论：信息安全体系应该是融合了技术和管理内容，并且充分考虑到人、流程和工具这 3 个因素综合作用的结构。这是从事信息安全建设工作最终希望看到的结果。当然，要促成蓝图的实现，信息安全实践者必须有一套得力的操作流程，基于先后关联的一系列关键活动来实现信息安全体系蓝图。本书对此做了详细论述。

本书对企业网络个人计算机安全、服务器安全和网站程序安全等，通过各行业检测评估实例进行了详细的讲解。对网络管理员比较关心的大型网络的入侵响应、犯罪取证及入侵事件的调查过程，作了全面的流程分析及操作，以使网络管理员改掉不良习惯，把安全风险减小到最低限度。通过阅读本书，网络管理员一定能更加有效地对网络进行安全加固和维护。

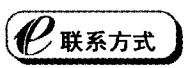
本书由郭鑫、崔红霞、姜彬编著。

本书适合从事网络安全的专业人员、网络管理员和设计人员阅读。

本书难免有些不当之处，甚至错误，欢迎读者直接致函作者，我们表示衷心地感谢！

最后，感谢所有支持、帮助过我们的人！

编 著 者



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

目　录

第1章 网络安全基础

学习网络安全，首先要了解一些关于网络安全方面的常识。因此，本章介绍网络常用的 IP 地址、端口、TCP/IP 和指令，以及网络专用名词解释，黑客入侵流程等，为学习网络安全技术打下坚实的基础。

1.1 认识 IP 地址

就像每个人都有一个身份证号码一样，网络里的每台电脑（更确切地说，是每一个设备的网络接口）都有一个 IP 地址用于标识自己。这些地址由 4 个字节组成，用点分十进制数表示及其 A，B，C 分类等。下面详细介绍 IP 地址。

1.1.1 什么是 IP 地址

在网络里，经常遇到 IP 地址这个概念。这是网络里的一个重要概念。所谓 IP 地址，就是给每个连接在 Internet 上的主机分配一个在全世界范围内唯一的 32 位地址。IP 地址的结构使用户可以在 Internet 上很方便地寻址。IP 地址通常用更直观的、以圆点分隔的 4 个十进制数字表示，每一个数字对应于 8 个二进制数的比特串，如图 1-1 如示。

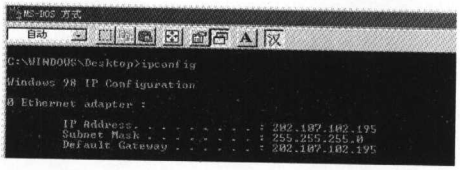


图 1-1 IP 地址

Internet IP 地址由 InterNIC（Internet 网络信息中心）统一负责全球地址的规

划和管理，同时由 InterNIC、APNIC、RIPE 这 3 大网络信息中心具体负责美国及其他地区的 IP 地址分配。通常每个国家需成立一个组织，统一向有关国际组织申请 IP 地址，然后再分配给客户。

1.1.2 IP 地址划分方法

IP 地址可以被划分成不同的类，根据最左边 4 个地址位的值决定具体的网络类型。例如，所有的 A 类网络地址最左边一位的值均为 0，而剩余 31 位的值既可以取 0 也可以取 1。即：

```
0xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
（x 代表 0 或 1，下同）
```

根据 A 类网络地址的规定，可以推算出该类型网络的有效地址范围是从 0.0.0.0 到 127.255.255.255。

B 类网络地址从左向右第一位必须为 1，第二为必须为 0，其他 30 位则可以自由取值。即：

```
10xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

因此，B 类型网络地址的有效取值范围是从 128.0.0.0 到 191.255.255.255。同样的，除第一位必须为 1 之外，C、D、E 类型网络地址的第二、三、四位都应当分别为 1。我们在表 1-1 中对不同网络类型 IP 地址的划分进行了总结。

表 1-1 IP 地址的划分

网络类型	特征地址位	起始地址	结束地址
A	0XXX	0XXX	127.255.255.255
B	10XX	128.0.0.0	191.255.255.255
C	110X	192.0.0.0	223.255.255.255
D	1110	224.0.0.0	239.255.255.255
E	1111	240.0.0.0	255.255.255.255

1.1.3 如何查询 IP 地址

经常有人问到如何查询 IP 地址。下面介绍两种方法。

第一种，通过网页来查询 IP 地址的所在地。这样的网页在网上有很多，比如 http://ip.loveroot.com/index.php。这里就可以通过 IP 来查询所在地。用 202.97.175.61 举例：进入该网页后，在“IP 地址”栏里键入想查找的 IP，然后单击【确定】按钮，就会显示出该 IP 对应的地址了，如图 1-2 所示。

第二种，利用专用的查 IP 软件，如国内最著名的查 IP 软件“追捕”。打开软件，在输入框里键入待查的 IP 地址 202.97.175.61，然后单击【追捕!】按钮，目标 IP 的数据就会显示在软件界面中，如图 1-3 所示。

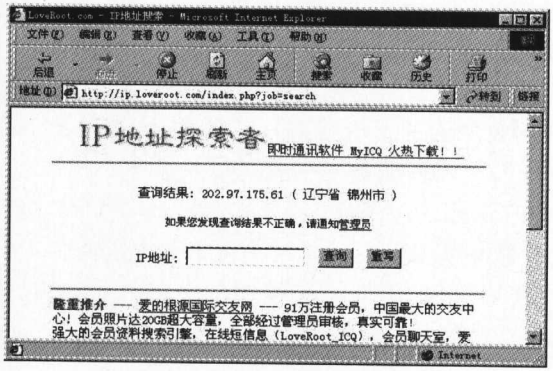


图 1-2　查 IP 地址网页

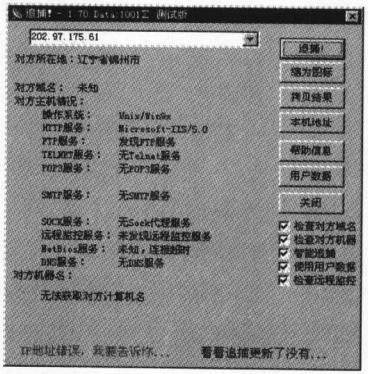


图 1-3　“追捕”软件界面

查看 IP 地址的方法还有很多，希望大家在熟悉上面两种方法的基础上，再去接触更多的方法。

1.2　端口

网民们上网的时候经常会遇到“端口”这个概念。那么，什么是端口，它在网络中又有什么意义呢？

先从 Internet 提供的一些常见的服务说起。

说到服务，首先要明白“连接”和“无连接”的概念。最简单的例子莫过于打电话和写信了。两个人如果要通电话，得首先建立连接——即拨号，等待应答后才能相互传递信息；最后还要释放连接——即挂电话。写信就没有那么复杂了，它是无连接的，正确的地址姓名等信息填好以后放入邮筒，收信人就能收到。

Internet 上最流行的协议是 TCP/IP。协议里对低于 1 024 的端口都有确切的定义，它们对应着 Internet 上常见的一些服务。这些常见的服务可以划分为使用 TCP 端口（面向连接，如打电话）和使用 UDP 端口（面向无连接，如写信）两种。

1．使用 TCP 端口常见的协议

- FTP：定义了文件传输协议，使用 21 端口。常说某某主机开了 FTP 服务便是文件传输服务。下载文件，上传主页，都要用到 FTP 服务。