羊羊不再沉默

Hacker防御实战手册

宋建龙 郑文鑫 马国平 编著

人民邮电出版社
POSTS & TELECOM PRESS

我不再沉默

Hacker防御实战手册

宋建龙 郑文鑫 马国平 编著

人民邮电出版社

图书在版编目（CIP）数据

羔羊不再沉默——Hacker 防御实战手册 / 宋建龙，郑文鑫，马国平编著；
—北京：人民邮电出版社，2004.9
ISBN 7-115-12620-8

I. 羔… II. ①宋…②郑…③马… 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（2004）第 099842 号

内容提要

本书是一本了解网络入侵技术、掌握入侵防御技巧的书。全书共 10 章，详细讲解了 WWW/HTTP/SMTP 等网络术语、常用的网络命令、端口解析、网络入侵基本方法、Windows 操作系统入侵、木马入侵、密码破解、DoS 攻击、网络炸弹、网络通信软件入侵、Web 服务器入侵以及相应的防御措施。

本书适用于对网络入侵、防御技术感兴趣的读者，也适合作为网管、网络技术员为提高系统安全性而使用的参考书。

羔羊不再沉默——Hacker 防御实战手册

◆ 编　　著　宋建龙　郑文鑫　马国平
◆ 责任编辑　马雪伶
◆ 人民邮电出版社出版发行　北京市崇文区夕照寺街 14 号
邮编　100061　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
读者热线　010-67132692
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销
◆ 开本：787×1092　1/16
印张：18.5
字数：446 千字　　2004 年 9 月第 1 版
印数：1-6 000 册　　2004 年 9 月北京第 1 次印刷

ISBN 7-115-12620-8/TP・4183

定价：28.00 元

前　言

进入21世纪后，网络与人们的生活越来越密不可分，换个角度来说，人们对网络的依赖性越来越强。虽然网络可以带给我们很多便利，如足不出户能知天下事、网上购物等。然而，有利必有弊，用户在网络上的一举一动很有可能已被不法分子监视上，轻则泄漏电脑的登录密码，重则被破坏者入侵。对于普通用户来说，这些攻击可谓是防不胜防，网络安全、黑客防御问题再次成为焦点。

黑客无处不在，黑客这一名词在计算机领域中更是“无人不知”。黑客们过硬的计算机编程功底、网络技术知识，对于广大计算机爱好者来说，有很多值得学习的地方。本书就以黑客为题材，针对现在各种黑客手段、入侵方法，介绍黑客入侵以及相应的防御方法。

本书的特点是：将现在主流的入侵以及防御方法，以图解的方式，一步一步地讲解，读者只需要通过相应章节即可轻松掌握入侵原理、入侵步骤，接着再通过每章中的相应防御技巧，确保自己电脑的安全性。

本书是一本了解网络入侵技术、掌握入侵防御技巧的书。全书共 10 章，详细讲解了WWW/HTTP/SMTP等网络术语、常用的网络命令、端口解析、网络入侵基本方法、Windows操作系统入侵、木马入侵、密码破解、DoS攻击、网络炸弹、网络通信软件入侵、Web服务器入侵以及相应的防御措施。

本书适用于对网络入侵、防御技术感兴趣的读者，也适合作为网管、网络技术员为提高系统安全性而使用的参考书。

在本书的编写过程中，得到了郑文鑫、芮锋等人的大力支持，在此向他们表示真诚地感谢。本书难免有疏漏之处，敬请作者批评指正，相关问题和建议可发送到我们的网站上http://www.easybase.net/lyb/，我们会以最快的速度回答大家的提问。

注：编写本书的目的是帮助大家更好地防范黑客攻击，确保自己电脑的安全。使用任何手段入侵他人电脑的行为均属于违法行为。

编者

2004年9月

目 录

第1章

防御必备知识

——黑客前传

黑客，一个既陌生又熟悉的名字，该名字时常浮现在每一位网民的脑海，尤如宇宙间的黑洞一般，既神秘又是那么地吸引人。相信每一位网民的内心对黑客都会有不同的概念，到底黑客是何方神圣呢？他如何利用网络解决各种各样的问题呢？在本章中，我们会掀开黑客的神秘面纱，让读者重新认识黑客。接着再介绍基本的网络术语、网络命令、端口等内容，通过这些内容，读者就可以更深入地了解黑客了。

通过本章，读者可以了解以下内容：

- 什么是黑客
- 基本网络术语
- 基本网络命令

1.1 黑客概述

黑客是英文“Hacker”的译音，而“Hacker”这个英文单词又来源于“Hack”，“Hack”本身有“砍”、“劈”等意思，也许正是因为这个英文单词的原意，不少网民认为“Hacker”就是干“砍”、“劈”这种事的人。然而事实并非如此，电脑中的“Hack”一词源于19世纪初。

在20世纪60年代，电脑正处于发展中的第二代。由于采用大量晶体管作为主要器件，所以一个完整的电脑系统是相当昂贵的，只有少数高等院校才拥有这些先进的设备。技术人员要使用这些先进的设备必须通过繁复的手续，再加上当时电脑的效率不高，为了绕过种种限制，进一步利用电脑，他们就编写了些捷径程序。虽然这些捷径程序必须依赖源程序，但是比源程序更简洁更完美，从而使得电脑工作效率大大提高。技术人员的这种行为当时就被称为“Hack”。由此看来，“Hack”并无贬义。

黑客（Hacker）这个名词出现于20世纪70年代的麻省理工学院。在大批高科技人才集中的理工学院实验室中，有不少精通电脑科学以及相关学科的人群，他们会借着网络共享资源，将大量的有用的知识无偿地授予有需要的人。他们这种精神，使人们想起了之前的“Hack”行为，“Hacker”就成为这群乐于助人、无偿奉献的高科技人才的代名词。

每种事物都会有两面性，由于黑客都具有过人的电脑、网络技术，他们会不停地创作一些捷径程序来提高电脑工作效率；但是，假如这些程序被所谓的“黑客”用于不法领域，这就会造成不可估计的损失。正因如此，不少人对黑客这一名词存在误解，事实上，真正的黑客绝不会随意入侵、破坏个人电脑或者商业电脑，那些自称为黑客并只会使用黑客前辈所创作的软件到处乱试、遇到难题自己又无法解决的人，绝对不配用“黑客”这个名字。

1.1.1 黑客前传

究竟怎样才算是一位黑客呢？黑客界的大哥大Jargon File给了一个较为广义的定义：只要你是一位行业中的精英，精通于该行业中的各种技术，并承诺热心帮助别人解决问题，具有克服种种限制的欲望，那么你就有可能成为黑客的一分子。

最初的黑客文化可以追溯到20世纪70年代初的第一台“微型电脑”的诞生，当时正是分时共享小型机以及ARPANet（Advanced Research Projects Agency Net）的实验期，一群专家级程序员、网络技术高手，创作了“Hacker”这个词，根据网络共享精神，共同建起了现在的Internet、创作了最严谨的UNIX操作系统，并使得Usenet运作起来，这些第一代的黑客使得World Wide Web成为今天的面貌，假如你是这个文化的一部分，并已经为它作了些贡献，而且圈内的其他人也知道你是谁并称你为一个黑客，那么你就是一名真正的黑客。

正如Jargon File所说，黑客精神并不局限于电脑网络领域中的黑客，只要你具有上述特点，为自己的行业做出贡献，并步入该行业的最高境界，通过黑客精神，帮助一切有需要的人，那么你也可以成为该行业的黑客。很显然，本书只是介绍电脑领域中的黑客，着重介绍黑客所需有技能以及所应具有的态度。

要成为一名黑客，必须先认同黑客们的为人态度。黑客会解决问题，创造有用的东西，信仰自由和双向的帮助，人人为我，我为人人。简单地说，成为黑客必须相信并做到以下事

情。

1．世界上存在着很多有待解决的问题

作为一位黑客是值得自豪的，这是因为他们经常可以体会到通过努力而解决难题所带来的快乐，成功的黑客在找到有待解决的问题的时候，他们会借助现有技术，运用自己的知识，开拓解决问题的新道路。在这个过程中，黑客们会感到无比兴奋。如果在遇到难题的时候就先打退堂鼓，那么将永远无法感受到成功的喜悦，请先给自己信心，努力寻找问题，努力解决问题。

2．无须为一个已解决的问题浪费时间

所谓时间就是金钱，而黑客们的时间、能力更是有限的资源，世界上还有其他有待解决的问题，没有必要在已解决的问题上浪费时间，哪怕对这个问题有不同的见解。同时，你也必须认识到，当成功解决一个问题时，请马上将有用的信息共享出来，让正在解决这个问题的其他黑客将精力集中在其他需要解决的问题上面。信息共享似乎成为今天黑客的道义。

3．拒绝无聊而单调的工作

黑客们不应该做一些简单而重复性的工作，这样会大大打击黑客的热情。黑客们应该投入到只有他们才能够完成的解决新问题的工作中。所谓大材小用就是这个意思，这种资源的浪费不但对黑客自己还会对其他人造成伤害。遇上无可避免而又必须做的无聊、单调工作时，黑客们应该创造出完成这种工作的捷径，使得这种工作变得自动化，“我为人人”就在这里体现出来了。

4．自由无价

作为一个黑客，不可因任何人而受到各种自由的限制。

5．态度非能力

作为黑客必须先具有黑客的态度，但是具有这些态度并不一定能成为黑客，所谓“No Pains，No Gains”，在保持黑客态度的同时，必须通过自己的智慧，不懈地努力，不停地提高自己的技能，并证明自己拥有过人的能力，这样才可成为真正的黑客。

1.1.2　黑客必备技能

正如上面所说，态度是必要的，但是技术才是重点，在成为黑客前，必须掌握足够的技术以应付日后解决难题的工作，黑客往往不是某个领域的专家，相反，他们必须拥有一套基本的技术，这些技术就是黑客必备技能。随着时代的进步，黑客们所需的必备技能也会略有不同，以下就介绍现在黑客所需必备的几项技能。

1．学会编程

编程也叫程序设计，这是第一项黑客必须掌握的技能。由于黑客在解决问题的时候不可能全部使用其他黑客创作的软件，这就无可避免地需要自己设计一个程序。当然，如果已掌握某一程序设计语言时，就已向黑客迈出了第一步。但是仅仅掌握一种语言还远远不能达到黑客所需的技术水平，必须掌握程序设计的方法、思路，这种方法、思路是独立于语言的。另一方面，必须有自学的能力，能够在几天内通过一些手册、结合以往程序设计的经验，迅速掌握一门新的语言，这就需要不停地学习、编程、学习、编程。现在的黑客都必须掌握 C/C++

这种核心语言，掌握这种语言是成为 UNIX 高手的必备条件。除此之外，还需要掌握 Perl、LISP 这两种语言。Perl 被广泛用于活动网页和系统管理，因此即便从来不用 Perl 写程序，至少也应该能读懂它；而 LISP 值得学习的原因是因为掌握了它就会得到丰富的经验，这些经验使你在以后的日子里成为一个更好的程序员，即使实际上可能很少使用 LISP 本身。

假如你是一位程序门外汉，可以从 Python 开始。它设计清晰，文档齐全，对初学者很合适。尽管它只是一门很好的初级语言，也同样非常强大、灵活，适合做大型项目。

2．在电脑中安装并维护一套免费的 UNIX 系统

要成为黑客，不仅要学会普通的 Windows 操作系统的安装与维护，还必须在电脑中安装一套免费的 UNIX 操作系统，如 Linux、BDS-UNIX 等。安装好这套系统后，还必须投入无比热情来学习使用与维护它。由于 UNIX 操作系统使用得最多的是命令行，所以必须抛弃传统的窗口使用习惯，老老实实地输入命令。为什么要掌握 UNIX 操作系统呢？这是因为 UNIX 操作系统不单只是一套免费的操作系统，而且它的源代码都是公开的。可以通过第一项技能，读懂操作系统程序，甚至修改操作系统程序，这样就可以帮助自己更方便地解决问题。

此外，UNIX 操作系统还是现在主流的 Internet 操作系统之一，如果用户连基本的 UNIX 指令都不懂，要成为 Internet 黑客简直是比登天还难。对于初学者来说（或者没有使用过 DOS 而直接进入 Windows 时代的用户），可以将 Linux 作为第一套学习的 UNIX 操作系统。由于 Linux 具有图形界面（如图 1-1 所示）、命令行界面，用户就可以更快地适应命令行界面。学会 Linux 的安装、配置、联网等基本知识后，就可以进入纯命令行界面，读懂系统程序并试着修改源程序了。

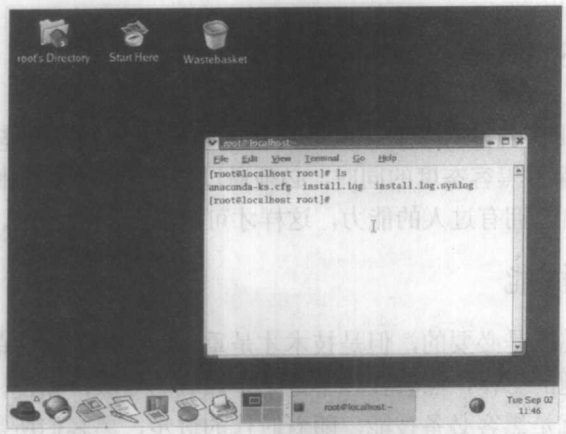

图 1-1　Linux 操作系统的图形界面

3．了解 World Wide Web 并掌握 HTML

黑客文化创造了 WWW（World Wide Web），但是并不等于这些由黑客文化创造出来的东西一定会用在黑客领域。作为一名黑客不可能只是使用浏览器浏览网页来解决问题，而需要掌握 HTML（Hyper Text Make-up Language）这种简单而实用的标记语言来编写基本网页，如图 1-2 所示。作为一名黑客，个人主页是不可少的，而这个主页应该体现出一定的价值，如提供一些免费源代码、帮助其他人解决问题等。

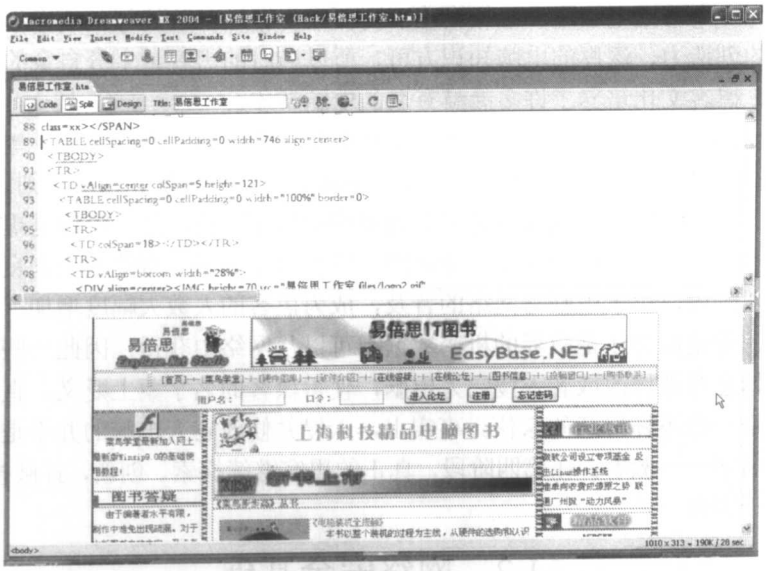

图 1-2　HTML 语言与它生成的网页

事实上，黑客文化与普通文化一样，要得到别人的尊重必须先尊重别人，所以应该尽量做到以下几点。

（1）编写免费软件或者提供免费源代码；

（2）测试、修改免费的源代码；

（3）提供有用的信息；

（4）帮助维护基础设施。

1.1.3　黑客攻击方式与类型

- 恶作剧型
- 隐蔽攻击型
- 定时炸弹型
- 矛盾制造型
- 职业杀手型
- 窃密高手型
- 业余爱好型

1.1.4　黑客发展史

黑客文化从 20 世纪 60 年代出现至今已有几十年，在这段期间黑客界发生过很多事情，为了使得读者对黑客有更深一层的认识，我们有必要回顾一下黑客的发展史。总的来说，黑客或者黑客文化的发展主要经历过如下 4 个阶段。

第一阶段：黑客发展的第一阶段是在 20 世纪 60 年代，当时的黑客为了提高昂贵电脑的工作效率，编写出各种程序。他们以程序设计为乐，逐渐形成了黑客文化的雏形。

第二阶段：20 世纪 60 年代末至 70 年代初是黑客发展的第二个阶段。由于当时电脑的普

及率不高，作为一个普通电脑用户已相当难，而要成为精通电脑的每一项操作的黑客，这就需要具有高度的创造力、深厚的电脑知识方可，所以当时的黑客是十分自豪的。经过黑客发展的第二阶段，黑客文化培养了许多赫赫有名的电脑奇才。

第三阶段：20 世纪 70 年代中期是黑客发展的第三个阶段。在这期间，黑客文化出现了“使用电脑不受限制”、“不得以任何方式修改、损坏电脑软件系统”这些准则。

第四阶段：20 世纪 80 年代以后是黑客发展的第四个阶段，这一阶段是黑客发展非常时期。为什么这样说呢？这是因为在前 3 个阶段，黑客这个名字一直给人带来良好的印象，但是自从进入第四阶段，由于电脑与网络的普及，成为黑客的人数大幅度增加。当时网络已应用于各大领域，无论商界还是政界的机密数据都可以从网络中获得，因此一些拥有黑客技术的“黑客”开始恶意地修改或者入侵它人电脑，使得黑客的名字蒙上贬义。直到今天，不少人还认为黑客是一些不怀好意的家伙。事实上，入侵并修改它人电脑的并不是真正的黑客，他们有另一个名字——骇客。在第四阶段，真正的黑客继续探索、创新，打破技术上的限制，让电脑资源归于民众。

1.2 网络安全基础

虽然现在网络已非常普及，即使是不太懂电脑的用户也可以轻松在网络中聊天、获取信息和娱乐等。但是对于网络基础、网络安全问题，大多数网民都只有一个淡淡的印象而已。在网络中接触到最多的就是 IP 地址、端口、WWW 和 TCP/IP 等名词，在这一节对这些内容进行详细的讲解。

1.2.1 WWW

WWW 是 World Wide Web 的简写，中文译为万维网或者全球网，而我们平时所说的 Web 或者 Internet 从广义上讲和它也是同一个意思。在没有 WWW 的时候，人们要在网络中传递信息，只能使用 E-mail、FTP 和 Archie 这几种方式。E-mail 可以使个人与个人或者个人与团体之间交换信息变得更方便；FTP 可以方便、安全、快捷地将文件在网络中传送；Archie 类似于现在的搜索引擎，可以在网络中查找所需的文件。虽然以上 3 种方式已经可以实现简单的信息交流，但是对于今天来说，这 3 种方式的信息交流太有局限性，用户必须获得对方的 E-mail 地址、FTP 地址、用户名和密码等方可进行信息交换。

除此以外，E-mail、FTP 和 Archie 这 3 种信息交换方式都会随着操作系统的不同而有不同的限制。为了解除这样或那样的限制，提高网络中的信息交换效率，我们就有必要开发出一种全新的并且独立于各种操作系统的信息交换方法。随着网络的发展，这种需求就越来越大。后来，日内瓦的欧洲粒子物理实验室 CERN（European laboratory for particle physics）开发出了超文本标记语言——HTML（Hyper Text Markup Language），这种标记语言是从一种称为标准化标记语言——SGML（Standard for General Markup Language）演化而来。HTML 的特点是简单易学，用户可以方便地将文本信息用 HTML 语言表示，如图 1-3 所示，并在互联网中传播。

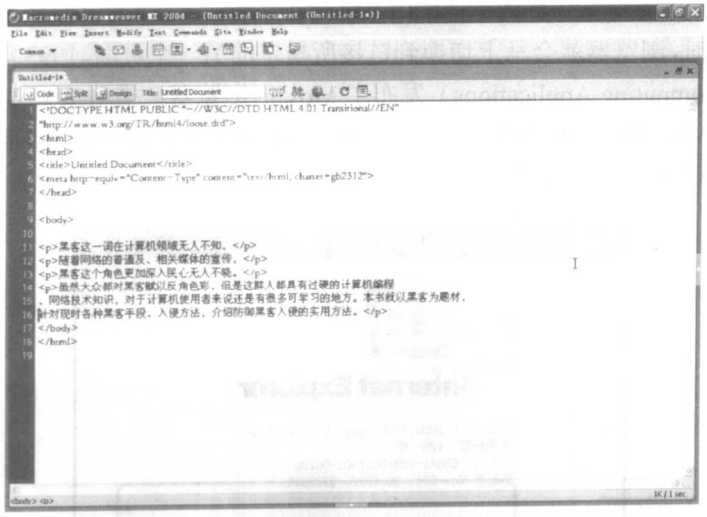

图 1-3　HTML 标记语言

为了在 Internet 中传播 HTML 文件，必须使用基于 TCP/IP 协议，这样 HTTP（Hyper Text Transfer Protocol）就诞生了。当这些必要条件都具备的时候，WWW 就正式出现了。WWW 通过 Web 服务器，解除了以前信息交流的限制，用户只需利用浏览器输入正确的地址，Web 服务器就马上以文本和图形的形式显示所需的信息，如图 1-4 所示。

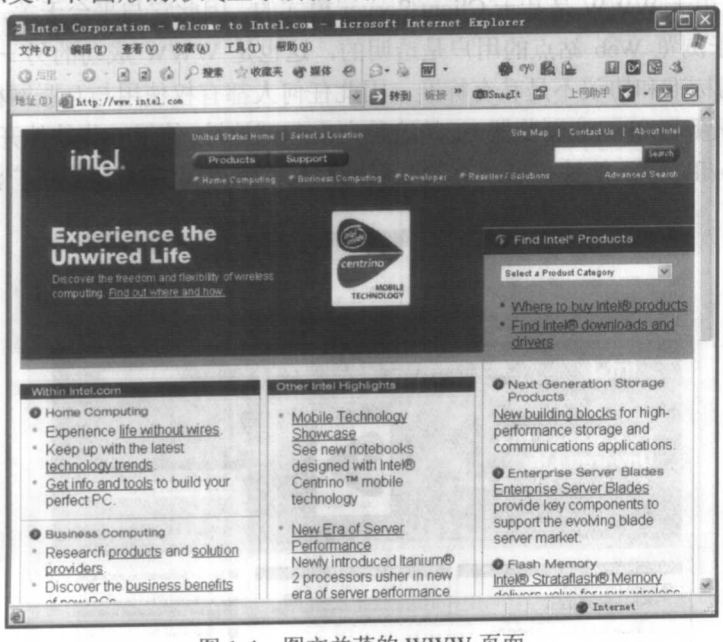

图 1-4　图文并茂的 WWW 页面

WWW 发展到今天，文本、图像、声音、影像以及交互式的应用程序都可统一到同一页面当中，WWW 已成为信息交换的一种很有效的方式。我们可以在 WWW 中浏览各种信息，并且通过页面中的超链接（URL），从一种信息来源转到另一种信息来源。所谓的超链接（URL，

Uniform Resource Location）是指一种指向 Web 页面的统一资源的定位器，当用户单击页面中的一个超链接时，浏览器就会马上切换到链接所指定的另一个页面。1993 年 NCSA（National Center for Supercomputing Applications）发布了 Mosaic 浏览器，推动 WWW 成为互联网中发布文本以及多媒体信息的一种必然手段。尽管现在 Mosaic 浏览器已绝迹，但是我们依然可以在现在的浏览器中找到它的踪迹，如图 1-5 所示。

图 1-5　IE 的产品说明

另一方面，由于 WWW 是基于 Client/Server 模式的，因此它与平台无关，如图 1-6 所示。通常 Server 对于浏览 Web 站点的用户是透明的，这也是 WWW 成功的另一个原因。CERN 所定义的互联网标准和协议不是私有标准，因此任何人都有权使用与互联网标准和规范一致的自己的 Web 服务器和 Web 浏览器。正是这种自由和开放性，使得一些软件开发商，如 Opera、Microsoft 和 Mozilla 等，能够扩展现有的互联网标准，满足 WWW 用户更广泛的需要。

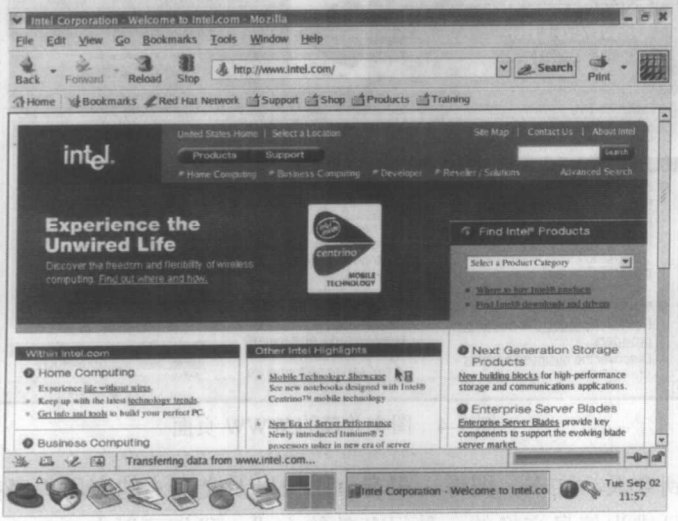

图 1-6　其他平台上的 Web 页面

1.2.2　TCP/IP

TCP（Transfer Control Protocol）/IP（Internet Protocol）是一种网络中最常使用的协议，该协议是由美国国防部开发的一种通信协议，允许不同的电脑共享网络上的信息。也就是说，通过 TCP/IP 协议可以将不同厂家生产的各种型号的电脑、安装着不同操作系统的电脑连接起来并互相通信。虽然原来 TCP/IP 协议的作用只是实现电脑间的通信，但是现在 TCP/IP 的作用已远远超出这个设想，它不再局限于 Internet 这个领域，在 Intranet 上也可使用 TCP/IP 协议，实现更安全、更方便的通信。

源于 20 世纪 60 年代末的 TCP/IP 协议到 20 世纪 90 年代已发展成为电脑间最常用的组网协议，这有赖于它的自身开放性；协议的组件定义及其多种实现方式都不用任何花费或花很少的钱就可以公开地得到，这使得它迅速成为 Internet 的基础协议。

网络是如何利用 TCP/IP 协议进行通信的呢？这就要从 TCP/IP 协议的网络模型来说明了。一般来说，TCP/IP 可以用一个分成 4 个层次的模型来描述，它们分别是链路层、网络层、传输层和应用层，如图 1-7 所示。

1．链路层

链路层也称为数据链路层或者网络接口层，在这一层当中包括操作系统中的设备驱动程序、电脑中对应的网络接口卡等。链路层将要发送的帧发送到线路中去，要接收的帧从线路中提取出来。

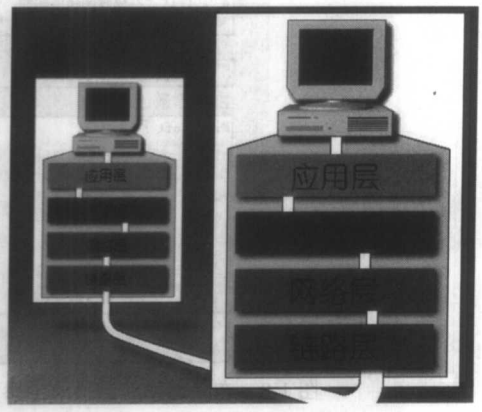

图 1-7　TCP/IP 模型

2．网络层

网络层也称为互联网层，这一层的功能是寻址、定址、数据打包和安排路径。在网络层有如下 3 种协议。

- Internet 协议（IP），它的基本功能是在主机和网络之间寻址、定址以及为数据包安排路径。
- 地址解析协议（ARP），用于获取位于同一物理网络中的主机硬件地址。
- Internet 控制信息协议（ICMP），发送关于数据包已送达的信息，也报告数据包传送过程中的错误信息。

3．传输层

传输层负责为两台主机上的应用程序提供端到端的通信。在 TCP/IP 协议中传输层可以使用以下两种协议。

- TCP。传输控制协议（TCP）为某些应用软件提供面向连接的、可靠的通信。这些应用软件通常需要一次传送大量数据，或需要一个对方收到数据之后发出通知。
- UDP（User Datagram Protocol）。用户数据报协议（UDP）提供无连接通信，因此不保证数据包将送达接收方。使用 UDP 的应用软件一般一次只传送少量的数据。应用软件