网络安全技术教程
——攻击与防范

黄鑫　沈传宁　吴鲁加　编著

中国电力出版社

内 容 提 要

本书分析目前常用的黑客攻击技术，并提出了相应的防御反击方案。作者为国内著名红客，多年从事网络安全工作。本书是他多年经验的总结，本书主要讲解了常见的黑客攻击技术、系统及网络隐患，以及如何预防黑客攻击。很多实例具有实战价值，可活学活用。

本书适合网络管理人员和对网络安全有兴趣的爱好者阅读。

图书在版编目（CIP）数据

网络安全技术教程——攻击与防范/沈传宁等编著. —北京：中国电力出版社，2002.5
ISBN 7-5083-1056-X

Ⅰ.攻… Ⅱ.沈… 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（2002）第 032892 号

中国电力出版社出版、发行
（北京三里河路 6 号 100044 http://www.infopower.com.cn）
汇鑫印务有限公司印刷
各地新华书店经售
*
2002 年 9 月第一版 2002 年 9 月北京第一次印刷
787 毫米×1092 毫米 16 开本 23 印张 569 千字
定价 33.00 元

前　言

现在，在互联网上最著名的搜索引擎 www.google.com 中敲入“黑客”这个词，可以查找到 484000 条信息，敲入“网络安全”这个词可以找到 261000 条消息。而敲入“电视”这个词，找到的信息总数为 675000。可见，黑客与网络安全随着互联网的发展，逐渐已经成为我们生活中密不可分的一部分。

对很多人来说，网络安全仍然是技术员的事，但毫无疑问的是，网络安全已经受到越来越多人的关注。而作为与网络安全密不可分的黑客技术也一直被媒体炒的沸沸扬扬。然而，涉及网络安全的技术的相关技术一直被认为是神秘而高深的技术。很多入侵系统的人在媒体的报道中往往都被称为“计算机天才”。这在一定程度上也吸引了很多年轻人的注意，他们纷纷效仿，希望能突破别人的安全系统，以证明自己也是一个天才，造成这一问题的根本原因在于人们对网络安全相关技术的不了解。

本书主要为那些对网络安全有所了解，并想掌握更多更全面的网络安全知识的读者所编写的。作者采用尽可能简单的方式向读者讲解涉及网络安全的一些技术的原理，希望读者在读完这本书后，能对网络安全的技术有进一步的了解，并体验到掌握知识的乐趣。

本书分 5 部分共 18 章，较全面介绍了涉及网络安全的各方面技术：

第一部分背景篇，介绍了作者对于黑客与入侵者的理解，并简单介绍了 TCP/IP 协议的基础知识。

第二部分基础篇，介绍操作系统与应用服务安全的相关知识。由于大部分读者接触较多的是 Windows 操作系统，因此该部分主要以 Windows 安全为主。

第三部分高级技术篇，向读者详细介绍了目前网络安全中一些高级技术，如电子欺骗、格式化字符串攻击技术的原理及相关知识。

而作为读者最有可能接触到的木马与病毒则单独作为第四部分进行讲解。最后的附录中向读者推荐了一些目前国际国内较知名的网络安全机构、组织及公司的站点。

最后要说的是：如果每个人把自己的经验、心得和熟知的部分写成文字，系统地讲给大家听，对这一领域的朋友们未尝不是好事，至少也算是一种对知识的回归，只要写出的文字能给志同道合的朋友带来启发，或者使初学者少走些弯路，我们也就心满意足、问心无愧了。

目　录

第 1 章　黑客与入侵者

1.1　互联网时代的问题

互联网的作用远远超过了我们的想像，现在，每天都有成千上万的企业、研究所和个人在上网。10 年前要建立起一个 Web 服务器并维护好这台服务器并不是一件很简单的事情，现在情况就不一样了，一个普通人就可以建立自己的 Internet 服务器。因为 Web 服务器的建立已经不需要掌握太高深的技术，大多数的操作系统在安装时默认都已经将 Web 应用服务软件装在机器上了。用户甚至不需要进行什么配置就能很好的运行起来。然而，这样的服务器虽然能良好的运行，却无法很好的保证安全性，因为绝大多数的维护人员都没有安全方面的经验。这样工作于危险状态的服务器数量每天都在增加，危机往往被忽视，人们强调的是上网的数量而不是质量。那么，为什么人们会对危险视而不见呢？

1.1.1　观念

计算机行业的厂商对公众进行误导，他们的市场营销人员总是异乎寻常的宣称他们产品的安全性，使普通消费者信以为真。事实上，根本没有哪个安全产品能确保用户的网络完全的安全。然而，过度的宣传某一类产品给用户造成了误导，让用户以为使用了这样的安全产品，就能解决网络的安全问题。一个简单的例子就是防火墙，不可否认防火墙在提高网络的安全性方面所做出的贡献，经过多年的推广，防火墙几乎已经成为网络安全的代名词，几乎所有的用户在被问到保护网络安全的方法是什么的时候，都会毫不犹豫的回答使用防火墙。防火墙的确是保护网络最基本的措施，但是，过度的宣传防火墙的能力，导致了用户对防火墙真实情况的不了解，甚至有的用户认为，安装了防火墙，自己的网络就安全了，不用担心了。事实并非如此，一个错误配置的防火墙可能根本不起任何作用。即使是完全正确配置的防火墙，也仍然有力所不能及的地方。需要让公众了解的是，网络安全不是一两个产品就能实现的，牵涉到方方面面的技术、产品。

1.1.2　损失

虽然我们的网络在快速地发展，用户不断地增加，不可否认的是，我国的互联网应用仍然是非常薄弱。大部分的企业往往是为了上网而上网，即使是建立自己的网站，也只是一个宣传的途径，放上几个页面，宣传一下自己的企业。并且可以在名片上印上自己企业的网址，使自己公司看起来还没有落伍。事实就是如此，也正因为这样，这些企业的服务

器即使受到了攻击，也不会有实际的损失，因为服务器上根本没有太多有价值的数据。而企业则因此对网络安全并不受重视。然而，这样的情况不会永远维持下去，我们的网络不可能永远停留这样的状态，现在就是一个大变革的时期，电子政务、电子商务正成为一个潮流。我们的每一个企业是否都需要等到网络攻击实际给企业造成了巨大损失时才去考虑网络安全问题呢？不！

1.1.3 系统复杂性

计算机界有一句经常引用的格言："80%的人只使用 20%的程序功能"。举一个简单的例子，在 Windows 98 操作系统中，有多少人能完全知道在 system 目录下那些众多的小软件的作用。Winpopup.exe，一个简单的消息发送接收的小软件，有多少人知道这个软件的作用并且了解它地使用方法，还有 Rundll32.exe、Rundll.exe、Ipconfig.exe 等等其他各种不同的小程序，他们的作用是什么？

同样，用户也很少知道他们所使用的操作系统内部运行情况，因为在大多数情况下，了解这些东西总是得不偿失。大多数人，出于工作需要或者通过专门的培训，才会去学这些关于操作系统的知识。

要跟上技术发展的步伐非常困难，软件工业是一个动态的环境，用户通常要落后开发两年。这种新技术与用户之间的矛盾就导致了安全问题。即使是 Windows NT/2000 操作系统被广泛应用的现在，能完全了解它所提供的各项服务都起什么作用的用户也不多。例如，服务是由系统缺省提供的，但用户并不知道这个事实。当那些服务被启用的时候，就会导致安全漏洞。然而，问题在于，用户并不知道这个情况，因此，当这样一台服务器被连接上网络时，就可能产生安全问题。

典型的例子有：

Windows NT/2000 中的为管理而设的共享；

一些服务的默认口令；

一些特殊的服务，如 Runas 等。

1.1.4 系统缺陷

有相当一部分的问题并非用户配置不合理所造成，而是因供应商本身产品开发存在缺陷，并且这样的问题是不受用户控制的。每天，都有新的安全漏洞被发现（Bugtraq 上每天都有大量的关于各种漏洞的讨论，平均每天有近 30 个左右的新安全漏洞被提交到 Bugtraq 的讨论区中，虽然最后被真正证实的漏洞数量只是提交的一小部分，但所发现的安全漏洞数量仍然非常惊人）。这些新的漏洞的信息通过各种方式递交给用户，例如邮件列表、Web 公告等。尽管如此，并不是所有的用户都能看到这些信息。

并且，由于开发商缺乏足够的反应能力，即使用户获得了关于漏洞的信息，但是缺乏相应的解决方案，导致用户无法修补这些系统，系统仍然处于危险的状态当中。虽然不可否认开发商的响应和解决方案是一个最佳的选择，但是用户不能错误地认为安全应该全部依赖于开发商。实际上，开发商从漏洞被公布到提供完全的解决方案需要一定的时间；甚

至在某些情况下根本就不能依赖开发商，例如开发商已经退出这方面的业务，不再提供对软件的支持。这时候，就需要用户能提出自己的解决方法。虽然不能说所有的安全漏洞都可以由用户来自己解决，但是绝大多数的漏洞都可以通过一定的处理来消除或者降低漏洞所带来的影响。而要做到这一点，需要用户对网络工具、安全漏洞以及各项相关的技术有一定的了解。

1.2 黑客与入侵者

1.2.1 认识黑客

你正在读这本书，相信你不会连黑客这个词都没听说过，黑客是由英文 Hacker 音译过来的名词。这个名词从诞生起就与网络息息相关，随着互联网应用的日益扩大，黑客这个名词被在媒体上出现的频率也越来越高，并且对黑客这个名词已经有了很多不同的解释：

黑客是一些技术天才，他们推动了计算机科技的发展；

黑客就是利用计算机进行犯罪的人；

黑客是一些以破坏别人的系统为乐趣的人。

尽管对黑客的看法各异，但目前在中国，黑客这个词带着明显的贬义，已经成为计算机系统破坏者的代名词。甚至只要犯罪中和计算机有一点关系，案件中的罪犯也常被媒体称为黑客犯罪。

黑客从英文 Hacker 翻译过来，hack 的原意是劈斩，做一件漂亮的事情。与计算机犯罪不同，黑客在诞生的早期，常是一个带褒义的词，他们推动了计算机的快速发展，为今天的互联网发展做出了不可磨灭的贡献。在其中诞生了很多今天鼎鼎大名的人物，如苹果电脑公司的创始人乔布斯、自由软件基金的创办人 Richard Stallman。《黑客的道德准则》一书中有一句话说，“通往电脑的路不止一条，所有的信息都应该是免费的，打破电子特权，在电脑上创造艺术和美，计算机将使生活更美好”。这充分说明黑客本身并不是破坏者。称计算机犯罪的人为黑客是对 Hacker 的本质并不了解，只会使用一些软件入侵系统的人根本就没有任何的资格与黑客这个词相提并论。

1.2.2 Hacker 文化简史

自从第一台计算机开始诞生起，计算机行业就成为了世界上最具吸引力的行业之一，不断地吸引世界上最优秀，最富有想像力的人才投入其中。最初的黑客是一些程序员，他们并没有称自己为 Hacker，他们以编写各种软件并且研究编程技巧为乐，并且逐渐形成了一套自己的文化。这些程序员对计算机的工作机制了如指掌，有精湛的程序开发技术，能熟练的使用 FORTRAN、汇编语言甚至是机器语言来编写应用程序。他们是 Hacker 时代的先驱者，默默贡献，却鲜为人知。

1961 年，当 MIT 出现了第一台个人电脑 DEC PDP-1 之后，这个时髦的科技玩具成为

培养 Hacker 的优秀工具。1969 年，美国国防部出于军事上的目的投资兴建了 ARPANET，ARPANET 是第一个横跨美国的高速网络，是今天 Internet 的原型。它的出现使得位于各地的研究人员能更好的实现交流，对于 Hacker 的发展也起到了至关重要的作用，网络将全世界的 Hacker 连接在一起，使得 Hacker 文化不断发展壮大。

另一个影响 Hacker 发展的重要因素是 Unix 的诞生，Unix 诞生在 AT&T 的贝尔实验室。它的作者是 Ken Thompson。这个操作系统最初是运行在一台报废的 DEC PDP-7 上的，作者写这个操作系统的目的只是为了运行自己开发的一个游戏。Unix 最初是用汇编语言开发的，而 Ken Thompson 的一位同事 Dennis Ritchie 在当时发明了一种新的程序语言，这就是今天被广泛应用的 C 语言。他们很快用 C 语言将 Unix 重写了一遍。并且，Unix 在随后的几年中成功地移植到数种机器上。这在当时是一个非常重大的进步，这意味着不需要为特定的机器写软件。而今天 C 与 Unix 的应用范围之广，出乎原设计者之意料，很多领域的研究要用到电脑时，他们是最佳拍档。到了 1980 年，Unix 已经被广泛应用到各大学与研究机构。

1975 年第一部 PC 出现，还有苹果电脑公司在 1977 年的成立，使得微机开始进入个人应用市场。随着微软公司 DOS 操作系统的诞生以及 IBM 新型廉价的 PC 机的出现，越来越多的人投身到计算机 Hacker 的世界，计算机的应用获得了快速的发展。

1992 年，一位芬兰赫尔辛基大学的学生 Linus Torvalds 在一台 386 PC 上开发一个类似 Unix 的操作系统内核，他把这个简单的操作系统的代码放到互联网上与大家共享，这个操作系统吸引了非常多的 Hacker，他们不断地对这个操作系统进行完善和扩充。借助互联网的帮助，一个类似 Unix 功能完整的操作系统 Linux 诞生了。它完全免费并且任何人都可以获得其中的程序源代码。Linux 最大的特色，不是功能上的先进而是全新的软件开发模式。在 Linux 被开发成功前，人人都认为像操作系统这么复杂的软件，非得要靠一个开发团队密切合作，互相协调与分工才有可能写得出来。而事实上，借助互联网以及全球 Hacker 的力量，Linux 很快全发展趋于成熟稳定，能与商用的 Unix 一分高下，渐渐有商业应用软件移植到 Linux 上。

Internet 在 20 世纪 90 年代获得了极快速的发展，伴随 Internet 而发展起来的 Hacker 也将成为互联网发展中新的亮点，他们将会成为推动 Internet 发展的重要力量之一。

1.2.3 入侵者与黑客的区别

Hacker 的产生源于网络，有一种不断探索的精神。它不仅仅是局限在计算机行业中，也可以在其他的领域中更好的发挥。在任何一门科学、任何一个领域中都有很多问题等待解决，旧的问题不断被解决，新的问题也不断出现。为了解决问题而不断学习，不断探索的态度才是 Hacker 的真谛。

为了与那些以入侵计算机系统而获得乐趣并且进行破坏的人区分开来，Hacker 将这些破坏者称为“Cracker”，中文翻译成“骇客”。骇客被认为是不负责任，没有同情心并且虚荣而自私。只知道对网络服务器进行恶意攻击来满足自己的欲望，不会有丝毫贡献。

而在现实社会中，以信息共享为核心的 Hacker 精神很难生存，出于商业利益的缘故，信息的共享是不会被商业社会所接受的。因此，Hacker 文化在今天的商业社会逐渐消失，

而 Cracker 反而借助互联网大行其道。而今天在公众的观念中，Hacker 与 Cracker 是完全一样的，而中文“黑客”则完全变成了网络破坏者的代名词。

1.3 安全现状

1.3.1 安全之难

随着互联网的发展，越来越多的政府机构、企业和个人将自己的计算机连接到了互联网上，特别是随着宽带技术的发展，很多的用户已经长期与互联网处于连接的状态。然而，用户的安全意识并没有与互联网一样的快速发展。其中最主要的原因是缺乏相应的安全培训，大部分连接在互联网上的用户对一些基本的安全常识都不是很了解，即使是一些企业和网站的管理员，也没有足够的安全知识来保护他们的系统的安全。虽然有些管理员通过自己的努力学习，对安全知识有一定的了解，知道修补一些系统的安全漏洞，但是与专心于研究入侵技术的入侵者们相比，维护网站的管理员们缺乏足够的精神来研究关于安全的问题。可以想像，对一个每天例行公事地做一些维护工作的网管的来说，这些例行的公事已经让他们非常的劳累，怎么会有激情去发掘网站的漏洞。大部分时候，网管的工作是在做一些亡羊补牢的事，当系统出现问题的时候，才去研究修补措施。这种做法不可能打造出一个安全的系统。

每天不断被发现的漏洞使得服务器总是处于不安全的境地，而互联网本身的开放性也从另一方面增加了这种不安全性。今天很多进行网络破坏的人，在互联网没有这么广泛应用的过去，并不会构成危胁。因为他们使用来进行入侵的工具、软件甚至是入侵的教材都来自开放的互联网，没有网络，他们也失去了存在的基础。

而信息安全涉及的领域相当的广阔，可以说，所有涉及到信息的保密性、完整性、可用性、真实性的相关技术都是信息安全所要研究的领域。也正是因为如此，要保护一个系统的安全、可靠需要掌握方方面面的知识。掌握这些知识本身就是一件困难的事。

1.3.2 安全之易

从传统的对 Hacker 的理解看来，他们都是一些有着高超的技术，对系统深入理解的人。这个理解在过去是正确的。然而，令人奇怪的是，这样的概念仍然被沿用至今。以至于很多的人学习攻击他人的计算机、窃取别人邮箱的口令只是为了让其他人认为自己很厉害。正是这一点简单的虚荣心促使他们到网上寻找入侵用的软件和文章，开始他们迈向所谓“黑客”的第一步。

任何人都把遭受攻击的损失怪罪到入侵者的头上，的确，入侵者对这些事件负有不可推卸的责任。可是，其他人有没有自己的责任呢。俗话说“苍蝇不叮无缝的蛋”，在受到损失时只会责怪别人是没有任何意义的。虽然现在网络上有很多的入侵行为，可是其中绝大

部分是没有什么技术含量的入侵，例如对口令的猜测，这是最常见的入侵行为。如果网管只是使用了一个简单的口令，使得系统被入侵，网管是否需要对入侵的后果负一定的责任。很多的入侵事件与人们思想上的松懈、法律意识淡薄、安全观念不强等是密切相关的。有绝大多数网络入侵是由于网络管理者或用户的不设防而导致的。即使是系统已经设置了安全防护措施，但人们却对此过于信赖，麻痹大意，缺乏必要的安全防范意识，从而给予入侵者可乘之机。实际的情况是，互联网上的很多服务器的口令都十分简单。

维护一个系统的绝对安全是非常困难的，但是要保证相对安全还是非常简单的。网络管理员需要应付的是那些数量众多的低层次攻击，这些攻击是针对系统最主要的攻击。几乎超过 90%以上的入侵行为都是一些技术含量非常低的行为，进行入侵的人很多都不具备太全面的计算机知识，他们只知道下载一个软件，或者下载一个漏洞的 exploit，然后运行发动攻击，很多甚至对利用的是什么漏洞、什么原理都不知道，这些人被称为“Script Kiddies”。网络管理员只需要有一个安全的口令，一个好的安全管理措施，并且经常给系统升级就能防御。

1.4 社会工程学

1.4.1 社会工程学概念

现实中发生的许多网络安全案例，破坏者使用的手法并不是十分的高明，仅仅是通过一些非常简单的技术对系统进行破解。如口令暴力猜测，这些攻击并不需要太高深的技术，仅仅使用一些现成的软件和一点耐心就能实现。甚至还有一种技术含量更低的破坏网络安全的方法，它通过种种手段来骗取操纵网络内部的人员提供必要的信息（如口令）来获取网络的访问权。这种操控电脑使用者而非电脑本身的方法被称为社会工程学。因为一个系统的安全设计无论如何出色，毕竟是由人来管理的，社会工程学就是利用的人们心理上的漏洞来对系统进行攻击的。

一个简单的例子：当用户收到发件人地址为 root@xxx.com 或 webmaster@xxx.com，第一印象就是，这是来自管理员的电子邮件。因为互联网上，webmaster、root 常常是网络管理员、系统管理员的账户名。然而，这些账户不是必须的，也就是说，没有什么法律规定 root 就是系统管理员，webmaster 就是网站管理员。并且电子邮件的发件人地址是非常容易伪造的，使用邮件地址并无法验证这是封来自管理员的邮件。尽管如此，对于一个没有太多安全意识的用户或一个没有什么经验的用户来说，这种方法仍然可能是非常有效的。

社会工程学源自现实中的社会，现实社会中的欺诈手段绝大部分可以借鉴到网络欺诈中。尽管这些方法很简单，很容易识破，但是这种欺诈手段仍然是十分有效的方法之一。只要现实社会中的欺诈行为没有消失，网络社会中的社会工程学就会依然存在。

1.4.2 社会工程学的应用

社会工程学不仅仅被利用来直接获得权限，在其他攻击方法中，有许多也间接利用了社会工程学。如常见的口令攻击，攻击者利用一些高速的口令猜测软件、一个庞大的字典文件对系统账户口令进行匹配。口令猜测容易成功与用户口令设置及字典的内容有关。由于许多系统用户没有设置安全口令的意识。往往使用一些不太安全的口令设置方式。如：生日、用户名+后缀、电话号码、英文单词、公司名称缩写等等。攻击者在口令猜测过程中会相应设置自己的口令字典。如猜测纯数字的口令时，先猜能组成生日的数字组合，对于98742516 这样不是生日的数字组合会放在较后面猜测或者根本不猜。这样，可以极大的降低口令猜测的次数，在较短的时间内将不安全的口令猜出来。

而很多流行的电子邮件病毒也同样利用社会工程学进行传播，典型的是流行邮件病毒“爱虫”，带毒邮件有一个非常诱人的标题，“I love you”，收到这个邮件的人往往都无法抗拒自己的好奇心而打开这封邮件。事实上，电子邮件病毒大都利用这类手法来传播，它们都有一个非常诱人的标题，如笑话、色情、奖金等，事实上，这是利用标题激起收件人的好奇心从而打开邮件。

1.4.3 社会工程学重要性

社会工程学在很多人眼中只是一个小把戏，对系统没有太多危害。也许你能做到不会被入侵者利用社会工程学进行破坏，但并不代表所有人都能。很多入侵系统的案例里，入侵技术并不高明，但是入侵者的确对用户的密码心理学非常了解。

然而很多网络管理员对此并不了解或者并没有相应的意识。几个月之前，我的一位朋友因为忘记了自己的一个邮箱的密码，于是打电话到提供服务的网络公司去寻求解决。令人吃惊的是网管只问了一下用户名，在其他的任何资料都没有进行验证的情况下就将这个用户名的口令改为空口令，然后告诉我的朋友可以使用了。虽然这是一个免费的电子邮件服务，不过从此之后我再也没有使用这个网站的电子邮件了。而且令人不安的是这个网络公司并非是一个小公司，而是一个非常著名的网络公司。

1.5 如何保证安全

关于如何才能保证安全的讨论曾经长时间充斥在网络上，极端的人认为对于安全漏洞和入侵技术的公开导致了目前互联网的不安全。可是如果保守漏洞的秘密不公开就能确保网络安全的话，这个安全本身就是建立在不牢靠的基础上的。漏洞和入侵的技术不被公开，并不代表漏洞就不存在，入侵的技术就会失效。信息是不可能封锁的，最终会被传播开来。而且通常情况下在入侵者中传播的速度要远快于网络管理员之间传播的速度。

不可能指望一个对安全知识不了解的管理员能维护好一个网络的安全，因为掌握网络安全相关的技术才是解决问题的最根本途径。对于一个系统管理员来说，除了需要有良好

的安全意识外，能熟练的掌握入侵者使用的技术和原理，对于维护系统安全的作用是不可估量的。入侵技术并不是什么神秘的东西，它只是我们传统计算机技术的一个延伸。从纯粹技术的角度来看，可以认为这些技术是社会的宝贵财富。技术本身是无所谓善恶的，这些技术掌握在入侵者手中，可能会给网络带来危害。但是不能因为这样就否定了技术本身。同样，这些技术被正确的利用，有助于维护网络的平稳运行，很多优秀的网络管理员本身对入侵技术就有深刻的了解。

第 2 章　TCP/IP 协议基础

通常提到的 TCP/IP 是指以 TCP 协议和 IP 协议为基础所构成的协议族。TCP（传输控制协议，Transmission Control Protocol）和 IP（Internet 协议，Internet Protocol）是目前使用最广泛的通信协议，以 TCP 和 IP 协议为核心所构成的 TCP/IP 协议族包括了数百种不同的协议。详细了解 TCP/IP 是一个艰苦的学习过程，本章并不打算详细讲述 TCP/IP 协议，只是为后面阅读本书提供一些必须的知识。如果希望对 TCP/IP 进行深入的了解，请阅读相关书籍。

2.1　TCP/IP 的历史

Internet 起源于美国与苏联这两个超级大国之间的冷战。60 年代初，美国国防部出于军事上的考虑，需要一种新型结构的网络。新结构的网络中的每一个节点都能独立工作，这样，在网络的其他部分遭到破坏后，未被破坏的部分仍然能正常工作。这个网络就是 Internet 的原型，当时称为 ARPANET。ARPANET 建立起来后，虽然能工作，但是仍然存在大量的问题，网络不够稳定、缺乏一个稳定可靠的通信协议的支持等等。

TCP/IP 协议就是在这样的背景下应运而生，TCP/IP 的诞生有着先天的优势。与其他的协议相比，TCP/IP 使用方便，实现成本低廉。并且，美国国防部在 TCP/IP 诞生后，向全世界无条件地免费公开 TCP/IP 协议的核心技术，使得 TCP/IP 也成为了一个开放性的协议。这些都直接促进了 TCP/IP 协议的发展，TCP/IP 很快成为了 Internet 通信的标准，TCP/IP 协议的广泛使用的同时也带动了 Internet 的发展。

今天，Interent 和 TCP/IP 已经不仅仅被用于军事上的目的，变得更加商业化，更加面向消费者。TCP/IP 已经被集成到几乎所有的操作系统中，它为不同的计算机之间的通信建立了一个稳定可靠的平台。

2.2　分层结构

网络协议通常分不同层次进行开发，每一层分别负责不同的通信功能。一个协议族，比如 TCP/IP，是一组不同层次上的多个协议的组合。与 OSI（开放式系统互联）的七层结构不同，TCP/IP 通常被认为是一个四层的协议系统，每一层都有各自的协议，实现不同的功能，如图 2-1 所示。TCP/IP 协议分四个不同的层次，分别是链路层、网络层、传输层和应用层。