“九五”国家重点电子出版物规划项目·希望计算机知识普及系列
网e新生活系列（6）

解读黑客

黑客是怎样炼成的

北京希望电子出版社　总策划
卢津榕　冯宝坤等　编　写

本版光盘内容包括:
本版电子书

北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

“九五”国家重点电子出版物规划项目·希望计算机知识普及系列
网e新生活系列（6）

解读黑客

黑客是怎样炼成的

北京希望电子出版社　总策划
卢津榕　冯宝坤等　编　写

本版光盘内容包括：
本版电子书

北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

内 容 简 介

在国际互联网几十年的发展历程中，来自黑客的侵扰已经成为我们不得不正视对待的一个安全问题，但什么是黑客，黑客又是炼成的呢？围绕这一系列问题，本版书展开了丰富细致的讲解。

本版书着眼于对黑客知识的全面介绍，重点则在于黑客攻防手段的详细解说，对黑客工具、网络漏洞、加密解密技术、防火墙技术等进行了全面的分析。全书由 12 章组成，内容包括：黑客的前世今生、防黑必读、黑客常见破解及攻击手段剖析、黑客工具大阅兵、常见系统漏洞全面解析、加密解密技术步步高、网络安全全面解决方案、黑客—接招、OICQ 功防手册、防火墙技术从入门到精通、密码功防实战、网络防黑和入侵检测产品大观等。

本版书具有技术内涵高、指导性强，内容新颖、丰富，涉及面广的特点。本版书不但是从事网络安全与管理的广大从业人员重要的指导书，同时也是高校相关专业师生教学、自学参考书和社会相关培训班推荐教材、各科研院所图书馆馆藏读物。

本光盘内容包括本版电子书。有关本书的技术和实际问题，请与作者联系，E-mail：fengbaok@public.tpt.tj.cn。

系 列 盘 书：网 e 新生活系列（6）
盘 书 名：解读黑客——黑客是怎样炼成的
总 策 划：北京希望电子出版社
文本著作者：卢津榕　冯宝坤　编写
CD 制 作 者：希望多媒体开发中心
CD 测 试 者：希望多媒体测试部
责 任 编 辑：马红华
出版、发行者：北京希望电子出版社
地 址：北京中关村大街 26 号，100080
网址: www.bhp.com.cn
E-mail: lwm@hope.com.cn
电话: 010-62562329,62541992,62637101,62637102,62633308,62633309（发行）
010-62613322-215（门市）　010-62629581（编辑部）
经 销：各地新华书店、软件连锁店
排 版：希望图书输出中心　周玉
CD 生 产 者：北京中新联光盘有限责任公司
文本印刷者：北京双青印刷厂
开本 / 规格：787 毫米×1092 毫米　1/16 开本　14.25 印张　328 千字
版次 / 印次：2001 年 6 月第 1 版　2001 年 6 月第 1 次印刷
印 数：0001-5000 册
本 版 号：ISBN 7-900071-32-6/TP・31
定 价：23.00 元（1CD，含配套书）

前　言

21 世纪是网络时代，“网络一家，四海一心”的概念早已经深入人心，越来越多的人开始相信：互联网将会改变我们的生活。不过，网络并不安全。在国际互联网几十年的发展历程中，来自黑客的侵扰已经成为我们不得不正视对待的一个安全问题。所谓黑客，其实就是那些利用技术手段，或者通过已有的黑客工具、自制工具等，对不知情的非本系统操作者进行攻击、扰乱、窥探甚至改变合法数据。究其实质，不排除有一部电脑高手以此来显示或者验证自己的编程技巧，但更多的黑客高手们是在自己的“黑程序”屡试不爽后铤而走险，最终以此为获得不法利益的犯罪手段。有道是“己所不欲，勿施于人”，又有一说，“魔高一尺，道高一丈”，要真正做到预防黑客入侵，就必须对黑客、黑客的工具进行测析，做到知己知彼，百战不殆。于是，经过几个月的精心策划、准备和制作，这本凝结了作者与编者心血的黑客之书终于如期与读者们见面了。

在编撰本书之前，笔者曾先后调察了许多电脑书刊的销售点和新华书店，发现目前仅有的同类书籍不是停留在简单介绍黑客概念、黑客理论的“高级阶段”，就是在黑客工具软件介绍、使用方面流于肤浅，缺乏系统性、可操作性，在内容上往往是每个问题都点到，而哪一个问题也没有说清、说透，整体内容显得较为零散，有拼凑的感觉。初学者看不懂，对高手则无甚帮助。在这种情况下，这样一本书就诞生了。

本书着眼于对黑客知识的全面介绍，重点则在于黑客攻防手段的详细解说，对黑客工具、网络漏洞、加密解密技术、防火墙技术等进行了全面的分析，即使读者是一位从未接触过黑客知识的非专业人士，或者您只是一位刚刚入门电脑的初学者，相信本书也会让您在电脑生活安全之路上有所收益。对编程高手、网络管理人员、网络安全检查和相关人员也会有所益处。读了就能懂，懂了就能用，这就是笔者策划本书的初衷。

本书由卢津榕、陈中杰、周锐、王雨田、唐天虹、正丰等人组织编写。但由于作者本身的水平有限，在短时间里为读者们奉上这样一本内容丰富的书籍，其中疏漏之处在所难免，也敬请广大读者批评指正。

冯宝坤

目　录

第一章 黑客的前世今生

本章重点

第一章作为本书的导入部分，其重点就是要向本书的读者概括都介绍一下黑客的由来、历史及特点，并由此澄清几个容易混淆的概念。通过这些介绍，让读者对黑客有一个感性上的全面认识，并引发深入了解的兴趣。

学习目的

全面了解黑客的概念、特点及相关技术背景，基本明确黑客所具备的条件。

如今，越来越多的计算机联入了Internet。作为当今规模最大的互联网络，Internet遍及180多个国家，容纳了60多万个网络，接入了2000多万台计算机，为1亿多用户提供多样化的网络与信息服务。

随着互联网的日益普及，人们对互联网的依赖也越来越强，网络已经成为人们生活中不可缺少的一个部分。但是，Internet是一个面向大众的开放系统，对于信息的保密和系统的安全考虑得并不完备，加上计算机网络技术的飞速发展，互联网上的攻击与破坏事件不胜枚举。计算机黑客犯罪已经渗入到政府机关、军事部门、商业、企业等单位，如果不加以保护的话，轻则干扰人们的日常生活，重则造成巨大的经济损失，甚至威胁到国家的安全。所以系统的网络安全问题已引起许多国家、尤其是发达国家的高度重视，不惜投入大量的人力、物力和财力来提高计算机网络系统的安全性。诸多种种，也就引发了本书的话题。

1.1 黑客?骇客?还是怪客

在正式开始本章之前，我们有必要先向读者澄清几个概念。不少人认为黑客就是在网络上非法侵入别人机器的人，但除了黑客外，我们还常常听到骇客、怪客的称呼，一些人也郑重其事地站出来，声称黑客与骇客是不一样的，他们声称黑客创造东西，而骇客只会破坏。另外，还有一些人也将那些只会破坏的入侵者称为怪客。

那么，究竟什么才是真正的黑客、骇客、怪客呢?

1.1.1 什么是“黑客”

事实上，黑客也就是英文“hacker”的音译，“hacker”单词源于动词“hack”，这个词在英语中有 “乱砍、劈、砍”之意，还有一个意思是指“受雇于从事艰苦乏味工作的文人”。“hack”的一个引申意义是指“干了一件非常漂亮的事”。在19世纪60年代的时候，电脑系统是非常昂贵的，都只是存在于各大院校与科研机构的“玻璃房”中，技术人员使用一次电脑，需要很复杂的手续，而且电脑的效率也不是很高。为了绕过一些限制，最大限度地利用这些昂贵的电脑，最初的程序员们就写出了一些简洁高效的捷径程序，这些程序往往较原有的程序系统更完善，而这种行为便被称为“hack”。在早期美国麻省理工学院中，“hacker”有“恶作剧”的意思，尤指那些手法巧妙、技术高明的恶作剧。可见，

至少是在早期，“黑客”这个称谓并无贬意。

“破解，不是学习使用一个什么软件，不是按照说明书来操作，它是一种人和人智力的较量，是一种智慧的战争艺术，是一种知识与知识的较量。从本质上讲，学习‘破解’跟学习其他知识一样。都是要下苦功夫，要靠灵感，要靠自己思考的。”这就是黑客们对自己行为的诠释。

1.1.2 什么是“怪客”与“骇客”

骇客、怪客是“cracker”的音译，就是“破坏者”的意思。这些人做的事更多的是破解商业软件、恶意入侵别人的网络并造成损失。

怪客具有与黑客同样的本领，只不过是在行事上有些差别而已，这也是我们常常很难分清黑客与怪客的原因之一。

其实，黑客也好，骇客、怪客也好，名称只是一种代号而已，应该说他们之间并无绝对的界限，我们也很难将他们区分得很清楚，他们都是非法入侵者。既是非法入侵，再区分什么善意入侵与恶意入侵也没有意义了，而且无论是哪一种入侵，无论是有意还是无意，都有可能造成被入侵者的损失。

1.1.3 怎样才算是一个黑客

首先，黑客绝非是自称的，自称为黑客，甚至只是取了一个与黑客相关的名字，都会遭到真正的黑客嘲笑。在黑客的圈子里，只有其他的黑客接待了你，得到其他黑客的认可，你才能算是个黑客。

其次，想做一名黑客，应该具有一定的创造力，仅仅是拿着黑客前辈们所编写的黑客软件到处乱试，一旦出现问题却又束手无策的人，绝对称不上黑客。

此外，一名黑客还应该具有黑客的精神以及黑客的行为，要能够融入黑客们自然形成的黑客文化当中去，才能算得上是一名黑客。

当然，不管怎么样，黑客的技能是必备的。

总的来说，要成为一名黑客，你必须是技术上的行家，并且热衷于解决问题，能无偿地帮助他人。

1.2 黑客简史

有一种观点，认为黑客对电脑技术的革新作出了不可磨灭的贡献，而近些年来互联网的飞速发展，也有黑客的一份功劳在其中。有些人对此观点嗤之以鼻，但我们只要回顾一下黑客发展的历史，就会发现这种说法并不过分。正如前文所提到的，“hacker”这个称谓在早期是令人自豪的，直到现在仍有人以被称为“hacker”（黑客）而自豪，并以洁身自好的姿态与“cracker”（怪客）们区分开来。的确，最早的“hacker”是一种褒义词，只有那些最优秀的技术专家，才能被冠以“hacker”的称号。这可以追溯到几十年前第一台微机刚诞生的时候。那时，因特网的雏形ARPANET刚刚建立，当时能够使用这个网络的，都是一些程序设计专家或是科学家等，总之都是一群处于高科技最前沿的人们，而正是这些人创造了“hacker”这个词。从某种意义上，可以把这些最早的“hacker”视为Internet

的创始人，正是他们开发出了强大的、迄今仍在作用的Unix操作系统，这就是最早的黑客。他们具有高超的技术、过人的智力，以及坚韧的探索未知事物的毅力。他们对电脑技术的发展，对因特网的发展，都作出了巨大的贡献。这些“黑客”是值得尊敬的。

到了70年代，情况发生了变化，更多的黑客出现了，这些黑客也同样具有高超的技术，他们以侵入别人的系统为乐，随意地修改别人的资料，使得黑客这个称谓逐渐变得不那么令人喜欢。同时因为大量的黑客及黑客技术的涌现，加上因特网的发展，让黑客与黑客之间交流更容易，在因特网上出现了专供黑客交流的BBS，黑客逐渐形成了科技领域，尤其是电脑领域的一个独特的群体。

1.3 黑客文化

黑客这个群体的相对人数绝对算不上多，但在信息时代的影响却绝不可小看，这些人往往掌握着最先进的技术，一旦他们要将这些技术用于不正当的用途，也就是所谓的“怪客行为”的时候，其危害是难以想象的。在黑客出现至今短短的几十年内，他们基本已经形成了自己独有的黑客文化。

要想了解黑客文化，我们可从黑客行为、黑客态度以及黑客们自己定下的黑客守则等几个方面来认识。

1.3.1 黑客行为

黑客们一再声称自己与“怪客”的不同，于是便对黑客行为有了各种各样的注释，但总结起来，不外乎以下几条：

（1）不随便攻击个人用户及站点。虽然黑客们在找到系统漏洞并侵入时，往往都会很小心避免造成损失，并尽量善意地提醒管理者，但在这过程中有许多因素都是未知的，没有人能肯定最终会是什么结果，因此一个“好的”黑客是不会随便攻击个人用户及站点的。

（2）常编写一些有用的软件。黑客编写的软件都是免费的，但又和一般的共享软件有所不同，因为这些软件的源代码同时也是公开的。

（3）帮助别的黑客测试与调试软件。没有人能写出完全没有一点错误或是不需要改进的完美软件，因而对软件的测试与调试是非常重要的。测试与调试软件甚至会比编写软件更耗费精力。但在黑客的世界中，这或许算不了什么，因为在编写出一个软件后，会有许多其他的黑客热心地帮助你测试与调试。

（4）义务做一些力所能及的事。黑客们都以探索漏洞与编写程序为乐，但在黑客的圈子中，除了探索漏洞与编写程序外，还有许多其他的杂事，如维护和管理相关的黑客论坛、新闻讨论组以及邮件列表，维持大的软件供应站点，推动RFC和其他技术标准等等，这些事都需要人来做，但也许并不都是那么令人感到有趣。所以，那些花费大量精力，义务地为网友们整理RAQ、写教程的黑客，以及各大黑客站点的站主，在网络上都是令人尊敬的。

（5）洁身自好，不与“怪客”混在一起。真正的黑客总是耻于与“怪客”为伍，他们不会随意破解商业软件并将其广泛流传，也不会恶意侵入别人的网站并造成损失。他们的所作所为更像是对于网络安全的监督。

1.3.2 黑客精神

（1）“free”的精神。“free”(自由、免费)的精神是黑客文化的精髓之一，“free”是黑客最应该具有的态度。黑客们诞生并成长于开放的互联网，他们解决问题并创造新的东西，他们相信自由并自愿地互相帮助。最明显的一个表现就是在互联网上，黑客们编写的各种软件都是完全免费共享的，甚至连源代码都是公开的。而黑客们在帮助你之后，唯一的要求只是你在成长起来以后同样地帮助别人。

（2）探索与创新的精神。所有的黑客都是喜欢探索软件程序奥秘的人。他们探索着程序与系统的漏洞，并能够从中学到很多知识，在发现问题的同时，他们都会提出解决问题的创新方法。

在互联网急剧发展，并在人们生活的方方面面起着越来越重要的作用的时候，正是黑客们的探索与创新精神，使得互联网的安全问题引起了人们的重视。

（3）反传统的精神。反传统的精神在黑客们身上表现得最明显不过了，不具备这种精神的人，很难想象他会成为一个黑客。而这里的“反传统”主要是指科学技术上的反传统，并不包含任何贬义。黑客们做得最多的事，就是探索与创新，这都需要他们具有反传统的精神。他们的快乐就源自于攻破传统的东西。

（4）合作的精神。个人的力量是有限的，黑客们很明白这一点，因此才有了那么多供黑客交流的论坛与新闻组。在技术上保守的人是不可能成为黑客的。

最后必须要说明的一点是，所谓的黑客精神不应该是想成为黑客的人所刻意追求的，这是在每一个黑客以及每一个即将成为黑客的人身上自发地表现出来的。

1.3.3 黑客守则

黑客崇尚的是自由，他们有组织，也都是一些松散的、为了讨论技术而存在的组织。而所谓的黑客守则，也不像是我们日常生活中的这样那样的以各种形式制定的守则，事实上，这是一群最崇尚自由的人，他们最不喜欢的就是规则，所以并没有绝对的黑客守则。但黑客对自己的技术都很自豪，不喜欢别人误解自己，也不喜欢别人将黑客与“怪客”、“骇客”之类混为一谈，因而在互联网上便流传着种种黑客们自律的“黑客守则”。

黑客守则有多种版本，比较典型的一种如下：

（1）不要恶意破坏任何的系统，这样作只会给你带来麻烦。

（2）不要破坏别人的软件或资料!

（3）不要修改任何系统文件，如果是因为进入系统的需要而修改了系统文件，请在目的达到后将它改回原状。

（4）不要轻易地将你要黑的或是黑过的站点告诉你不信任的朋友。

（5）不要侵入或破坏政府机关的主机。

（6）已侵入电脑中的帐号不得清除或修改。

（7）可以为隐藏自己的侵入而作一些修改，但要尽量保持原系统的安全性，不能因为得到系统的控制权而将门户大开。

（8）不要做一些无聊、单调并且愚蠢的重复性工作。

（9）做真正的黑客，读遍所有关于系统安全或系统漏洞的书。

1.4 黑客必须具备的基本技能

作为一名黑客，是需要一定技术深度的，虽然随着技术的发展，黑客们需要不断地学习，尝试使用更新更好的技术，但一些基本的技能应该是必须要掌握的。

1.4.1 程序设计基础

毫无疑问，编程是每一个黑客所应该具备的最基本的技能。

然而，黑客与程序员又是不同的，黑客往往掌握着许多种程序语言的精髓(或说是弱点与漏洞)。黑客们都是以独立于任何程序语言之上的概括性观念来思考一个程序设计上的问题。汇编语言、C语言都是黑客们应该掌握的。

黑客们培养这种能力的方法，也与常人有所不同，他们也看种种书籍，但更多的是读别人的源代码，这些源代码大多数是前辈黑客们的作品，同时他们也不停地自己写程序。

1.4.2 了解并熟悉各种操作系统

Unix之所以如此受到黑客们的重视，并不仅仅因为它最初就是由黑客所编写的。我们知道，除了Unix外还有很多操作系统，但能得到源代码并能够任意修改的操作系统，只有Unix! 更重要的是，Unix是用于网络的操作系统，互联网上有很多主机使用的操作系统都是Unix，至少在目前，互联网还不能没有Unix。因此，许多黑客同时也是一个Unix专家，他们清楚Unix这个操作系统的整个运作过程与基础。

除Unix操作系统外，黑客还必须熟知诸如Linux，Windows和Novell等操作系统，才能让自己做黑客如虎添翼！Windows 98操作系统属性对话框见图1-1。

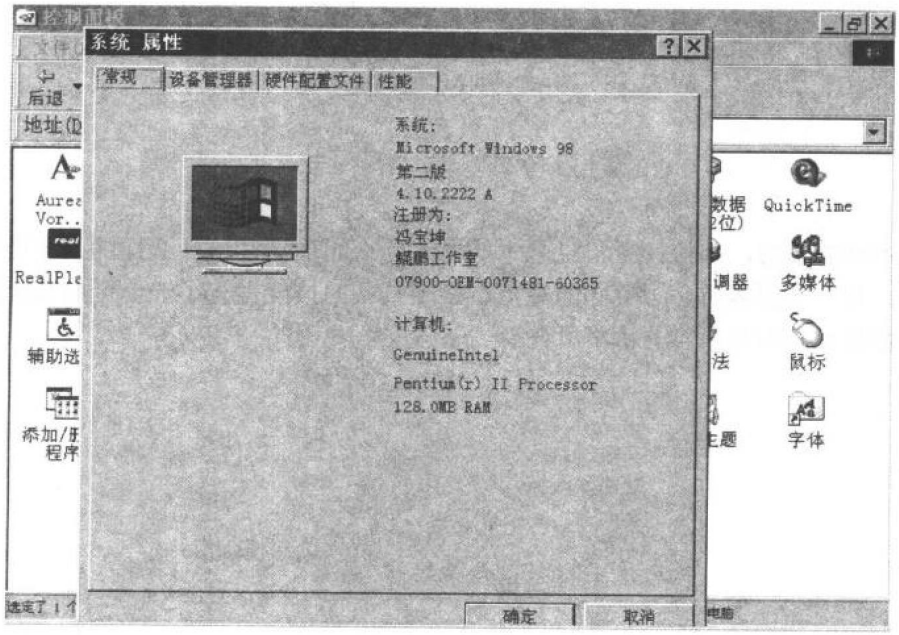

图1-1 Windows 98操作系统

1.4.3 互联网的全面了解与网络编程

黑客们所创造出来的东西，在很多领域都在起着作用，但只有互联网，才是黑客们真正的舞台。作为一名黑客，不懂得使用World Wide Web与HTML（HTML编辑利器见图1-2）是不可思议的。同时，若没有网络编程基础，要做黑客也是无从谈起。

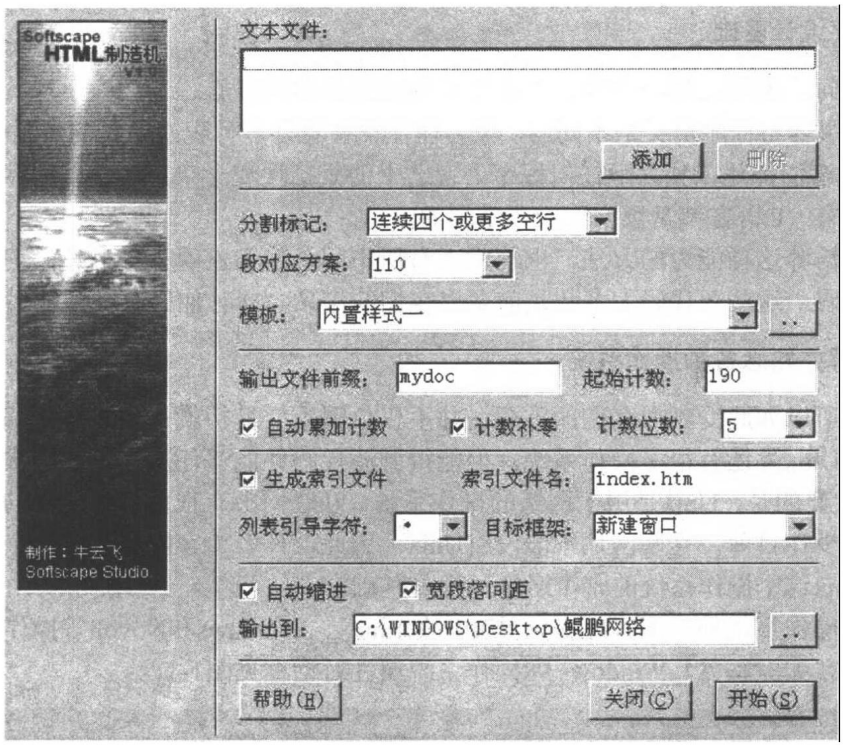

图1-2 HTML编辑利器

1.5 本章小结

通过本章的学习，相信读者已经基本明白了什么叫作黑客，什么样的人才能够成为黑客。同时，对一名黑客所必须遵守的规范、必须具备的技能等有了一个全面系统的掌握，而这些内容也正是本章内容的精华所在。

第二章 防黑必读

本章重点

本章在详细阐述与系统安全相关的网络概念的同时，重点介绍了远程攻击及防范、缓冲区溢出漏洞产生与防范等问题。

学习目的

深入了解防黑特别是网络防黑的相关概念及部分应急处理方法。

2.1 基本概念解析

在正式进入本章的内容之前，我们有必要面对这样一个现实：你的电脑真的安全吗？特别是对于许多网络用户而言，他们知道他们面临着一定的威胁。但这种威胁来自哪里、究竟有什么后果，他们并不十分清楚。就让我们先来了解一下您正在面临的威胁。

一般来说，对普通的用户来说，面临的安全性威胁主要有以下几个方面：

（1）病毒问题。这是广大用户最了解的一个安全问题。计算机病毒程序很容易做出，有着巨大的破坏性，其危害已被人们所认识。从前的单机病毒就已经让人们谈毒色变了，如今通过网络传播的病毒无论是在传播速度、破坏性和传播范围等方面都是单机病毒所不能比拟的。

目前全球已发现 5 万余种病毒，并且还在以每天 10 余种的速度增长。有资料显示，病毒威胁所造成的损失，占网络经济损失的 76%，仅“爱虫”发作在全球所造成的损失，就达 96 亿美元。

一般谈到病毒问题还包括特洛伊木马（Trojan Horse）和蠕虫（Worms）问题。他们虽然不是严格的病毒，但不仅和病毒的危害性相当，而且一般也会伴随着病毒一起向用户发起攻击。特洛伊程序一般是由编程人员编制，它提供了用户所不希望的功能，这些额外的功能往往把预谋的功能隐藏在公开的功能中，可掩盖其真实企图。蠕虫则是一个或一组程序，它可以从一台机器向另一台机器传播；与病毒不同的是，它不需要修改宿主程序就能传播。

（2）非法访问和破坏（“黑客”攻击）。黑客攻击已有十几年的历史。黑客对于大家来说已经不再是一个高深莫测的人物，黑客技术逐渐被越来越多的人掌握和发展，目前，世界上有 20 多万个黑客网站，这些站点都介绍一些攻击方法和攻击软件的使用以及系统的一些漏洞，因而系统、站点遭受攻击的可能性就变大了。尤其是现在还缺乏针对网络犯罪卓有成效的反击和跟踪手段，使得黑客攻击的隐蔽性好，“杀伤力”强，是网络安全的主要威胁。而黑客活动几乎覆盖了所有的操作系统，包括 UNIX、Windows NT、VMS 以及 MVS 等。黑客攻击比病毒破坏更具目的性，因而也更具危害性。Yahoo!、Amazon 等国际著名网站被黑事件早已不是新闻。据统计，全球平均每 20 秒就有一个网站遭到黑客攻击。

（3）管理的欠缺。网络系统的严格管理是企业、机构及用户免受攻击的重要措施。事

实上，很多企业、机构及用户的网站或系统都疏于这方面的管理。据 IT 界企业团体 ITAA 的调查显示，美国 90%的 IT 企业对黑客攻击准备不足。目前，美国 75%-85%的网站都抵挡不住黑客的攻击，约有 75%的企业网上信息失窃，其中 25%的企业损失在 25 万美元以上。此外，管理的缺陷还可能出现系统内部人员泄露机密或外部人员通过非法手段截获而导致机密信息的泄漏，从而为一些不法分子制造了可乘之机。

（4）网络的缺陷及软件的漏洞或“后门”。因特网的共享性和开放性使网上信息安全存在先天不足，因为其赖以生存的 TCP/IP 协议，缺乏相应的安全机制，而且因特网最初的设计考虑是该网不会因局部故障而影响信息的传输，基本没有考虑安全问题，因此它在安全可靠、服务质量、带宽和方便性等方面存在着不适应性。此外，随着软件系统规模的不断增大，系统中的安全漏洞或“后门”也不可避免的存在，比如我们常用的操作系统，无论是 Windows 还是 UNIX 几乎都存在或多或少的安全漏洞，众多的各类服务器、浏览器、一些桌面软件等等都被发现过存在安全隐患。可以说任何一个软件系统都可能会因为程序员的一个疏忽、设计中的一个缺陷等原因而存在漏洞，这也是网络安全的主要威胁之一。

基于这些现实，怎么解决这些与我们息息相关的网络安全问题？有道是“知己知彼，百战不殆”，让我们先从概念入手，把“防黑工作”从入门到精通。

2.1.1 万维网(WWW)

WWW即World Wide Web，中文一般称为万维网(或全球网)，平常说的Web和互联网其实与此是同一含义。创建WWW是为了解决Internet上的信息传递问题。在WWW创建以前，几乎所有的信息发布都是通过E-mail，FTP，Archie等实现的。E-mail的使用让不同的团体和个人之间的信息交换变得很广泛；FTP(文件传输协议)用来从一台计算机到另一台计算机进行文件传输；Archie（意为“公用软件文件查询系统，为FTP在线查询数据库；提供了全球匿名FTP程序目录）用来查找Internet上的各种文件，由于Internet上的信息散乱地分布在各处，因此除非知道所需信息的位置，否则无法对信息进行搜索。

由于这样或那样的限制，必须开发出一种全新的独立于各种平台的方法，以便于在Internet上传递信息。正是在这种需求下瑞士日内瓦的欧洲粒子物理实验室CERN开发出超文本标记语言(HTML)。HTML是从一种称为标准化标记语言(SGML)的文档格式语言演化而来的。HTML设计为易于学习、使用和在Internet上传递信息的一种文档表示语言，HTML比SGML更简单易学。为了在Internet上传递HTML文档，要使用基于TCP/IP的协议。这种协议后来成为超文本传输协议(HTTP)。WWW是随HTTP和HTML一起出现的，Web通过使用强有力的媒介传递信息，克服了许多早期信息传递的限制。Web服务器利用HTTP传递HTML文件，Web浏览器使用HTTP检索HTML文件。从Web服务器一旦检索到信息，Web浏览器就会以静态和交互(如文本、图像)的形式显示各种对象。

随着文本、图像、影像、声音和交互式应用程序的统一，WWW已经成为信息交换的一种很有效的方式。正是由于WWW的出现，我们才可以浏览各种信息来源，并且通过各种超级链接从一种信息来源转到另一种信息来源。超级链接是指向Web页面的统一资源定位器(URL)的对象。当用户单击一个超级链接时，该用户就会到超级链接所指向的Web页面。URL可以看作是Web页面的地址。每个Web页面都有一个或多个URL与之相关。在特殊应用程序和浏览器的推动下，Web很快成为Internet上发布文本和多媒体信息的一种有效手段。

WWW很大程度上是在NCSA（National Center for Supercomputing Applications）于1993年发布Mosaic（Web浏览器）后得到普及的。

WWW之所以如此流行，是因为它克服了Web浏览器出现之前许多应用程序的缺点，这些应用程序在Internet上用来发布信息。在Web浏览器出现之前，Internet上几乎所有信息都是字符文本格式，这样的信息不能按照多种格式表示，导致了浏览和搜索方面的困难。而WWW上的信息可以有多种格式，易于浏览和理解。例如，在讨论复杂问题时，可以使用图表、影像剪辑甚至交互式应用程序，而不仅仅是字符文本，这样会便于解释论题，使人一目了然。WWW集成了所有的视觉辅助效果来表示信息。

由于WWW是基于客户机/服务器模式，因此它是与平台无关的。通常，服务器对于浏览Web站点的用户是透明的，这是WWW之所以成功的另一个原因。CERN所定义的Internet标准和协议不是私有标准，因此任何人都有权使用与Internet标准和规范一致的自己的Web服务器和Web浏览器。这种自由和开放性使得一些机构（如NCSA，Netscape和Microsoft）能够扩充现有的Internet标准（如HTML），满足WWW用户更广泛的需要。正是这些先驱机构的努力，才使得WWW一直成为Internet的首选信息发布工具，为Internet的使用者提供了更多的选择和控制权。

与其他信息发布工具相比，WWW由于所需的费用很低，并且覆盖面广，因而具有很大的吸引力。另外，使用各种搜索机制和Web站点分类目录数据库注册一个Web站点，可以使客户在需要时得到所需的信息。

2.1.2 TCP/IP协议

一名成功的黑客，必然要对TCP/IP有透彻的了解，这是任何一个有能力的入侵者所必备的素质。只有深刻理解了TCP/IP协议，才会知道Internet是怎样运转的。而事实上TCP/IP协议的应用领域已不仅仅限于Internet，比如说，可以利用TCP/IP建立Internet（见图2-1）。

TCP/IP协议是由美国国防部开发的一组通信协议，允许不同的计算机共享一个网络上的信息。当把两个相同的PC联网已不再是一个技术性的挑战时，TCP/IP提供了解决下面这个棘手问题的办法：那就是如何将一台Pentium PC连接到一台DEC小型机或Silicon Graphics工作站上去。事实上，TCP/IP协议是使Internet各部分紧密结合的粘合剂。

下面我们分别介绍TCP与IP的意义。

TCP

TCP也就是英文Transfer Control Protocol的缩写，意为“传输控制协议”。

TCP是可靠的、基本的传输协议，用于提供可靠的、全双工的虚拟线路连接。连接是在发送和连接的节点端口之间实施的。TCP的数据流是8位一组的，它可在TCP主机之间提供多个虚拟线路的连接。

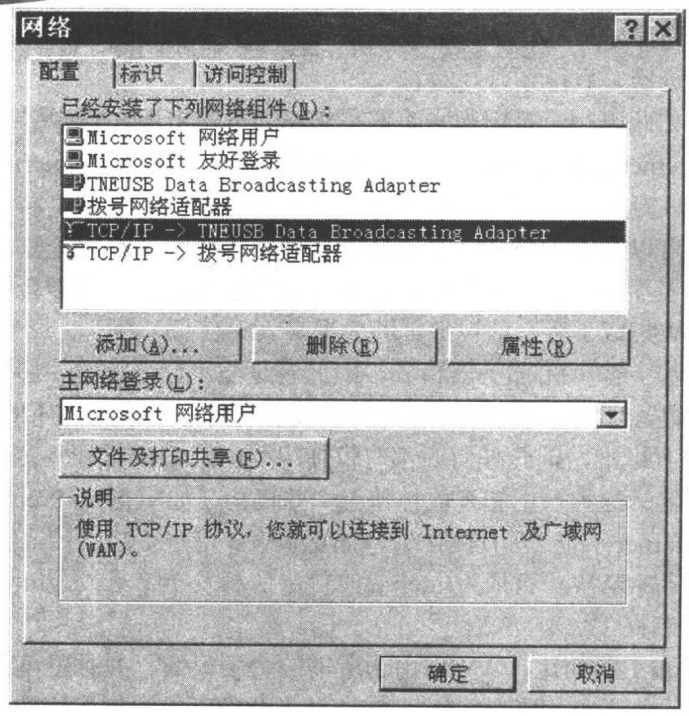

图2-1 TCP/IP协议

IP

IP是英文Internet Protocol的缩写，意即“互联网协议”。

IP协议是一个网络层协议，它在许多数据链路层协议上提供无连接数据服务。但是IP协议同其他网络层协议一样，不负责数据仓库的传送，它尽最大的努力传送数据。而上层协议可以在IP协议的基础上负责数据仓库的传送服务。IP提供了一系列有趣的服务，成为设计其他协议的基础。IP提出独立于下层的网络逻辑地址（即IP地址）来表示。它利用地址决议协议（ARP）把这一逻辑地址同一个节点的物理节点地址联系起来。

TCP/IP可以提供比其他协议更大的便利，其中之一就是上面所提到的，可以在各种不同的硬件和操作系统上工作，因而利用TCP/IP可以迅速方便地创建一个子网络。这类网络中可以有Mac机、IBM兼容机、Sun工作站、MIPS机等。这些机器可以用共同的协议与同伴进行通信，正是由于这个原因，传输控制协议（TCP）和互联网协议（IP）的应用越来越广泛。TCP/IP现在已经成了连接不同系统的共同标准。在网络普及的美国，TCP/IP处于公共领域，并且美国国防部要求在安全部门及其所属的承包商、研究单位和大学中使用，几乎所有的计算机系统销售商都提供TCP/IP。

互联网技术屏蔽了底层网络硬件细节，使得不同类型的网络之间可以互相通信。但TCP/IP协议组本身存在着一些安全性问题。由于大量重要的应用程序都以TCP作为它们的传输层协议，因此TCP的安全性问题会给网络带来严重的后果。

目前还没有十分简便的方法防止伪造IP地址的入侵行为，但我们可以采取以下措施来尽可能地保护系统免受这类攻击。首先，我们可以配置路由器和网关，使它们能够拒绝网络外部与本网内具有相同IP地址的连接请求；而且，当包的IP地址不在本网内时，路由器