电脑报 东方工作室

黑客来袭

HACKER

主编：尚北京

网络安全常用命令、软件使用方法

简单的攻击手段

常见的恶意攻击和防范方法

寻找和利用漏洞

木马、病毒、防火墙和入侵检测

攻击原理和程序设计方法

黑客攻击手段的具体应用

重庆出版社

黑客来袭

编　著：尚北京

重庆出版社

图书在版编目（CIP）数据

黑客来袭 ／尚北京主编.—重庆：重庆出版社，2002

ISBN 7-5366-6031-6

Ⅰ.黑… Ⅱ.尚… 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（2002）第091156号

编　　著：尚北京

责任编辑：刘庆丰

封面设计：黄　河

黑客来袭

重庆出版社出版、发行

新华书店经销

重庆升光电力印务有限公司印刷

*

开本：787×1092　1/16　印张：17　字数：408千

2003年1月第1版　　2003年1月第1次印刷

印数：1～5 000

*

ISBN 7-5366-6031-6/TP·103

定价：22.00元

作者简介

尚北京，1982年1月生于北京市，现兼职于北京时达网苑技术有限公司。

1990年开始接触电脑并受到中国计算机协会副会长田文柱先生的启蒙教育，对电脑知识有了强烈的渴求，1992年购买电脑并开始学习，小学期间曾多次获得各级比赛奖项，于1993年荣获北京市电脑雏鹰奖章。

1996年首次发表文章于报刊，随后发表频率日渐增多，先后成为《移动信息》、《北京青年周刊》、《网友》、《大众电脑》等刊物技术版面特约撰稿人，《网络报》“网络安全”和“懒汉技巧”等栏目主持人。

1998年有幸拜入北方工业大学马述教授门下，开始学习计算机编程和网络安全等热门知识，从此便逐渐对网络安全产生了浓厚兴趣。同年组建了“坐井观天”、“源代码堆栈”等安全网站，并加入Mudfrog黑客组织（红岩黑客组织前身），后成为该组织核心成员。

1999年通过计算机等级考核认证，担任《网络报》报社技术员。并与张跃（《计算机世界》网络工程师）建立了“堆栈”黑客组织，组织成员一度达到近百人，同绿色兵团、红色力量等黑客组织共同进行过多次网络安全“交流”活动。

2001年考入北京石油化工学院，同时成为“简单游戏”网站安全部技术负责人，并兼职北京时达网苑技术有限公司网络管理员。在不断的学习过程中主要发表过《网络安全初步》、《高等数学与黑客学》等较具代表性文章。同年11月被《数字生活》杂志推举为“数字精英”。

2001年8月在《网络报》编辑赵巍（网名Moonstone）、《数字生活》杂志技术编辑孙磊（网名Yagami）、《网友》杂志编辑凌佳奇（网名云雀）、主编马侠麾（网名风妖）、恒基伟业工程师林兴陆（网名小林）等人的帮助下开始编写《攻学兼防》一书。

前　言

FORWARD

互联网的繁荣使更多的人开始关注、接触并使用网络，然而网络与现实社会一样存在着各种危险，上网者的个人资料可能被泄漏、使用的系统可能遭受攻击、在网络上可能受到各种欺骗……黑客与电脑病毒在网络上几乎随处可见。作为一名刚刚使用网络的人来说，面对如此多的危险要想保护个人隐私和系统的安全就显得非常困难了。但是我们面对网络真的不堪一击吗？事实并非如此，大多数人是因为没有安全意识或者安全意识薄弱才受到攻击的。

此外，网络安全作为随网络一同产生的一个知识领域，并不单单是黑客和系统管理员所重视的话题。对于任何使用网络的人来说，学习网络安全就好比生活中要普及法律知识一样必不可少，对黑客攻击方法的了解，既可以使我们免受攻击，还可以对我们学习电脑知识中有所帮助。几乎所有的黑客知识都是深化的电脑理论知识和纯熟的操作技术的完美结合，因而对于这方面知识的学习可以使我们的技术大有长进。

《黑客来袭》正是沿着防范黑客攻击、学习黑客知识的主线出发，从网络安全的基本话题讲起，逐渐展开、深化，由浅入深地介绍网络上可能造成危害的途径以及相应的防范、解决方法，读者在阅读过本书之后便可以初步掌握安全上网的方法，并学会一些常用软件的应用，同时理解黑客思想，并了解常见的黑客攻击的手段和内幕。

由于本书的写作时间较长，从2001年8月起笔至今已近一年，虽然中途作过多次修改，但网络的瞬息万变必然是传统出版物无法超越的，因此这样看来过多地介绍流行技术并不能给读者带来更多的益处，然而使用比较经典的内容又显得过于千篇一律，因而作者配合自己在学习网络安全中的一些心得体会，着重于有关黑客思想和黑客方法上。黑客思想是一种考虑问题特殊性的思维方式，掌握了这种思想才是学习网络安全的关键，读者在掌握了这种思维方式之后，便可以在网络上获取更加具体的内容进行学习。

由于作者水平有限，书中错误难免，望读者给予指正、批评。作者希望在网络安全的学习道路上能与您共同进步。

内容提要

从内容和文章深度上看，本书可以分为三个学习阶段：

第一章至第三章为初级阶段，主要介绍网络安全的基础理论和常用命令、软件的使用方法，了解简单的攻击手段，网络上比较常见的恶意攻击和防范方法等内容。读者在完成本阶段的学习之后可对黑客技术和网络安全内容有感性了解，同时体会出黑客思想。

第四章至第八章为中级阶段，主要介绍漏洞的寻找、利用。当读者明白了漏洞对于黑客的重要性之后，继续学习有关木马、病毒、防火墙和入侵检测等较为深入的章节，这是网络上最常见的攻击与防御的方法，无论技术上如何变革，对于黑客和防御者来说，他们所进行的各种操作都是由上述几个方面构成并发展而来的。

第九章至第十章为高级阶段，阅读第九章需要有一定的编程基础，该章主要涉及的程序都是前面部分中的一些程序的简化版本，主要阐述攻击原理和程序设计方法，第十章为黑客攻击手段的具体应用、比较经典的攻击过程等介绍性内容。

全书采用章节目的编排次序，节内容都相对独立，章之间有一定的依赖次序，总体上呈现循环前进式编排，这有点类似传统武术中的“境界”，读者在阅读过一个章节后，可能会对前面所学内容有全新的认识和体会，逐渐深入地了解网络安全知识。

此外本书有两个附录，汇编了著名的黑客组织和软件的简介和相关地址，供读者查阅、学习。

书中部分章节参阅了其他书籍，并且在很多热心网友的协助下完成，作者特在此列出相关的参考书目，并对下列人员的支持与帮助表示由衷的感谢：

1.参考书目：

《黑客教程》高志国 龙文辉编著

《程序员》2001年合订本

《C程序设计》谭浩强著

《TCP/IP网络管理》王晓东等译

2.鸣谢人员：

小容 著名网络安全软件开发程序员

小林 恒基伟业工程师

与天为敌 安络网站系统管理员

目录

第1章 基础知识与理论

本章将从一些基本的网络安全术语开始揭开黑客神秘的面纱。平时总会听到一些电脑高手口中念念有词，那么他们所说的话究竟是什么含义呢？在不断的学习过程中，必不可少的是同其他学习者进行交流，尤其在网络上，与高手交谈不能将主要精力集中在思考对方词语的含义，而应该体会对方的思想，因此基础理论的扎实与否直接关系到今后学习的效率。

此外本章还会对网络的发展和结构作一些介绍，让读者明白自己身处的网络发展阶段和黑客技术在网络结构中的位置，明白网络欺骗、攻击、病毒程序、信息监听等黑客技术在网络结构中的层次位置。这样才能真正明白攻击和防御的含义。

1.1 网络安全术语解释

1.1.1 协议

网络是一个信息交换的场所，所有接入网络的计算机都可以通过彼此之间的物理连接设备进行信息交换。这种物理设备包括最常见的电缆、光缆、无线WAP和微波等，但是单纯拥有这些物理设备并不能实现信息的交换，这就好像人类的身体不能缺少大脑的支配一样，信息交换还要具备软件环境，这种“软件环境”是人类事先规定好的一些规则，被称作“协议”，有了协议。不同的电脑可以遵照相同的协议使用物理设备，并且不会造成相互之间的“不理解”。

这种协议很类似于“摩尔斯电码”，简单的一点一横，经过排列可以有万般变化，但是假如没有“对照表”，谁也无法理解一份杂乱无章的电码所表述的内容。电脑也是一样，它们通过各种预先规定的协议完成不同的使命，例如RFC1459协议可以实现IRC服务器与客户端电脑的通信。因此无论是黑客还是网络管理员，都必须通过学习协议达到了解网络运作机理的目的。

每一个协议都是经过多年修改延续使用至今的，新产生的协议也大多是在基层协议基础上建立的，因而协议相对来说具有较高的安全机制，黑客很难发现协议本身存在的安全问题直接入手进行网络攻击。但是对于某些新型协议，因为出现时间

短、考虑欠周到，也可能会因安全问题而被黑客利用。

对于网络协议的讨论，更多人则认为，现今使用的基层协议在设计之初就存在安全隐患，因而无论网络进行什么样的改动，只要现今这种网络体系不进行根本变革，就无法从根本上杜绝网络黑客的出现。但是这种黑客技能已经超出了本书的范围，因而不在这里详细介绍。

1.1.2 服务器与客户端

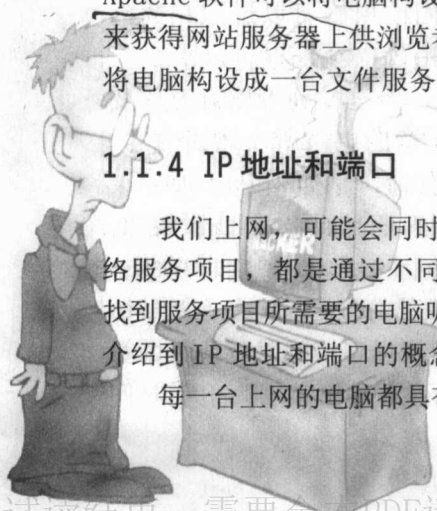
最简单的网络服务形式是：若干台电脑作为客户端，另使用一台电脑当作服务器，每一个客户端都具有向服务器提出请求的能力，而后由服务器应答并完成请求的动作，最后服务器会将执行结果返回给客户端。这样的协议很多，例如我们平时接触的电子邮件服务器、网站服务器聊天室服务器等都属于这种类型。另外还有一种连接方式，它不需要服务器的支持，而是直接将两个客户端电脑进行连接，也就是说每一台电脑都既是服务器、又是客户端，它们之间具有相同的功能，对等完成连接和信息交换工作。例如DCC传输协议即属于此种类型。

由此看出，客户端和服务器分别是各种协议中规定的请求申请电脑和应答电脑。作为一般的上网用户，都是操作着自己的电脑（客户端），并且向网络服务器发出常规请求完成诸如浏览网页、收发电子邮件等动作的。而对于黑客来说则是通过自己的电脑（客户端）对其他电脑（有可能是客户端，也有可能是服务器）进行攻击，以达到入侵、破坏、窃取信息的目的。

1.1.3 系统与系统环境

电脑要运作必须安装操作系统，如今流行的操作系统主要由UNIX、Linux、Mac、BSD、Windows 2000、Windows 95/98/Me、Windows NT等，这些操作系统各自独立运行，它们有自己的文件管理、内存管理、进程管理等机制。在网络上，这些不同的操作系统既可以作为服务器，也可以作为客户端被使用者操作，它们之间通过“协议”来完成信息的交换工作。

不同的操作系统配合不同的应用程序就构成了系统环境，例如Linux系统配合Apache软件可以将电脑构设成一台网站服务器，其他使用客户端的电脑可以使用浏览器来获得网站服务器上供浏览者阅读的文本信息；再如Windows 2000配合FTPD软件可以将电脑构设成一台文件服务器，通过远程FTP登录可以获得系统上的各种文件资源等。



1.1.4 IP地址和端口

我们上网，可能会同时浏览网页、收发电子邮件、进行语音聊天……如此多的网络服务项目，都是通过不同的协议完成的。然而网络如此之大，我们的电脑怎么能够找到服务项目所需要的电脑呢？如何在一台电脑上同时完成如此多的工作的呢？这里就要介绍到IP地址和端口的概念了。

每一台上网的电脑都具有独一无二的IP地址，这个地址类似于生活中人们的家庭地