Crack The Hacker
狙击黑客

——黑客攻防技术见招拆招

武新华
李秋菊 等编著
陈艳艳

超大容量DVD教学光盘

赠送45讲教学视频，总计281分钟

- ★ 黑客其实并不神秘（视频录像:13分钟）
- ★ 揭秘扫描、嗅探与欺骗（视频录像:41分钟）
- ★ 系统漏洞的入侵与防御（视频录像:4分钟）
- ★ 揭秘木马和间谍软件（视频录像:36分钟）
- ★ 斩断伸向QQ和MSN的黑手（视频录像:30分钟）
- ★ 代理与日志的清除（视频录像:38分钟）
- ★ 远程控制技术大集合（视频录像:33分钟）
- ★ 留后门与清脚印（视频录像:3分钟）
- ★ 黑客入侵防范技术（视频录像:30分钟）
- ★ 备份升级与数据恢复（视频录像:13分钟）
- ★ 打好网络安全防御战（视频录像:40分钟）

清华大学出版社

内 容 简 介

本书以较详实的内容和浅显易懂的语言，介绍了黑客攻击计算机的一般方法、步骤，以及所使用的工具，并向读者详细讲述了防御黑客攻击的方法，使读者在熟悉基本网络安全知识的前提下，掌握基本的反黑知识、工具和修复技巧，以便在遇到别有用心者的入侵时能够尽可能做到心中有数，从而采取相关的方法来制定相应的自救措施，而不是茫然无措，不知如何应对。

在本书附带的多媒体教学光盘中包含了大量全程多媒体视频讲解，紧密结合书中内容和各个知识点，采用情景化教学、详细图文对照以及真实场景演示等方式进行了深入讲解，在扩充本书知识范围的基础上，有效地弱化了本书的学习难度并大大激发了读者对黑客技术的学习兴趣。

本书内容丰富，图文并茂，深入浅出，适用于广大网络爱好者，同时可作为一本速查手册，适用于从事网络安全的人员及网络管理员。

图书在版编目（CIP）数据

狙击黑客——黑客攻防技术见招拆招/武新华，李秋菊，陈艳艳等编著. —北京：清华大学出版社，2008.6

ISBN 978-7-302-17451-6

I. 狙… II. ①武… ②李… ③陈… 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（2008）第 056330 号

责任编辑：钟志芳　朱　俊
封面设计：范华明
版式设计：赵丽娜
责任校对：王　云
责任印制：杨　艳
出版发行：清华大学出版社　　地　　址：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　邮　　编：100084
社　总　机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：北京密云胶印厂
装 订 者：北京国马印刷厂
经　　销：全国新华书店
开　　本：185×260　印　张：21.5　字　数：475 千字
（附 DVD 光盘 1 张）
版　　次：2008 年 6 月第 1 版　　印　　次：2008 年 6 月第1 次印刷
印　　数：1～5000
定　　价：38.80 元

前　言

尽管当今的网络已经在逐渐地改变着人们的思维方式及生活习惯，但大多数人的网络安全意识还很匮乏，在遇到别有用心者的入侵时还不知道如何应对。因为网络“黑客”的存在，人们往往是谈“黑”色变，“黑客”的侵袭会造成很多意想不到的情况发生，例如，在我们正在为精彩的网页着迷时，突然硬盘狂响不止，最后发现所有的程序都不能运行了；正在给网友写 E-mail 时，突然弹出一个对话框，上面写着“我是幽灵，我要毁了你的电脑！”；正在聊天室里与网友激情聊天时，突然弹出一堆对话框，无论怎么关都关不掉，最后只能无奈地重启计算机；正在登录 QQ 时却突然提示密码错误，试遍所有可能的密码却依然不能通过……

越来越多来自网络的“信息垃圾”、“邮件炸弹”、“病毒木马”、“网上黑客”等威胁着网络的安全，如何能够让广大电脑用户在尽可能短的时间内，了解黑客的起源、常用工具以及攻击方式，并在熟悉基本网络安全知识的前提下，掌握基本的反黑知识、工具和修复技巧，让广大用户对网络安全高度重视起来，从而揭开黑客的神秘面纱，采取相关的方法来制定相应的自救措施呢？

本书正是基于此目的而特意编写的，全书的主线就是黑客的“攻与防”，告诉读者应该如何建立个人电脑的安全防护措施，从此使自己远离黑客攻击的困扰，确保自己电脑数据的安全。学习本书后，可以使读者在实际应用中碰到黑客攻击时，能够采取相应的措施来防御，做到“胸有成竹”。

我们不提倡那些肤浅的入侵、进攻以及破坏，那些都是真正的黑客所鄙视的。本书最主要的精髓在于：读者学习后能够运用本书介绍的黑客攻击和防守方法，去了解黑客，进而防范黑客的攻击，使自己的网络更加安全。

本书围绕“攻与防”展开叙述的同时，特别注重实练案例的演示作用，针对每一种攻防手段，都尽量结合实际的例子来进行介绍，以使读者能够对这些黑客的攻防技术有更加感性的认识。

本书还配有超大容量 DVD 教学光盘，赠送 45 讲教学录像，贯穿到每一章，让读者像在课堂上听课一样轻松掌握，即使您是电脑新手也能通过视、听、看的互动方式，以最快的速度高效率地实现各种操作，全面确保您的网络安全。

本书由众多经验丰富的高校教师编写，具体编写情况是：李防负责第 1、2 章，段玲华负责第 3 章，陈艳艳负责第 4、5、6 章，柳勇良负责第 7 章，李秋菊负责第 8 章，武新华负责第 9、10 章，王英英负责第 11 章，安向东负责第 12 章，曹燕华负责第 13 章，最后由武新华统审全稿。本书在编写过程中还得到了许多热心网友的支持，并参考了大量来自网络的资料，对这些资料进行了再加工和深化处理，在此对这些资料的原作者表示衷心的感谢。

由于作者水平有限，书中的疏漏之处在所难免，恳请广大读者批评指正。

最后，需要提醒大家的是：

根据国家有关法律规定，任何利用黑客技术攻击他人的行为都属于违法行为，希望读者在阅读本书后一定不要使用本书中介绍的黑客技术对他人的电脑进行攻击，否则后果自负。

编　者

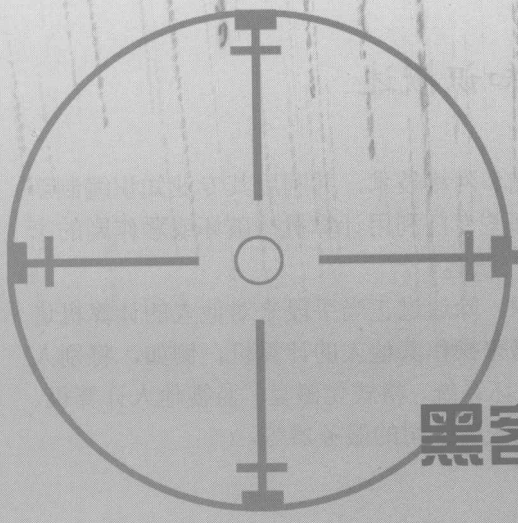
2008 年 2 月

目　录

Crack The Hacker

狙击黑客

——黑客攻防技术见招拆招



第1章

黑客其实并不神秘

重点提示

★ 黑客基础知识概述

★ 黑客的专用通道：端口

★ 黑客常用的入侵命令

本章精粹

通过本章的学习，读者可对端口扫描、扫描工具的使用方法及黑客常用的入侵命令等有一个基本了解，这些内容是成为一个黑客必须掌握的。

随着互联网对人们日常生活影响的深入，人们的生活已经很难离开网络。与此同时，网络的安全问题也引起了人们的高度关注。而黑客则是网络世界中很神秘的一类人，他们有时会义务去维护网络的安全，有时却又以网络破坏者的形象出现。本章将揭开黑客的神秘面纱，并对与他们有关的常用知识进行初步介绍。

1.1　黑客基础知识概述

黑客（Hacker）的原意是指那些精通操作系统和网络技术，并利用其专业知识编制新程序的人。但到了今天，黑客一词已被用于泛指那些专门利用计算机搞破坏或恶作剧的家伙，对这些人的正确英文叫法是 Cracker，故又称“骇客”。

这些人往往具有非凡的计算机技术和网络知识，除通过正当手段来对他人的计算机进行物理性破坏和重装系统外，他们还可以通过网络来操作其他人的计算机，例如，将别人的计算机当跳板来盗取另一台计算机内的文件、破坏系统、格式化磁盘、监视他人计算机、偷窥他人隐私、远程控制他人计算机、入侵攻击他人或公司的服务器等。

1.1.1　为什么会受到黑客入侵

其实，许多时候，大多数黑客进行攻击的理由都很简单，大体存在如下几个方面的原因。

（1）想要在别人面前炫耀一下自己的技术，例如进入心仪女孩的机器上去修改一个文件或目录名，算是打个招呼，不但给其一个惊喜，也会让她对自己更加崇拜。

（2）看不惯一些人的做法，可又不便当面指责，于是攻击他的电脑，更有甚者获得他的隐私，在适当的时机揭其老底，令其难堪。

（3）好玩、恶作剧、练功。这是许多人，其中包括学生，入侵或破坏网络的主要原因，除了有练功的效果外，同时还有一种网络探险的刺激。

（4）窃取数据。偷取入侵的主机硬盘中的文件或各种网上密码之后，从事各种商业应用活动，甚至恶意偷窃银行存款等。

（5）抗议与宣示。这是敌对国、敌对势力之间最常出现的黑客行为，例如 2001 年 5 月中美黑客大战，两国的黑客互相攻击对方网站，双方均有数千计的网站遭到攻击，轻者被篡改主页面，严重者则整个系统遭到毁灭性的打击。

1.1.2　全面认识 IP 地址

在网络上，只要利用 IP 地址都可以找到目标主机。因此，如果想要攻击某个网络主机，首先就要确定该目标主机的域名或者 IP 地址。所谓 IP 地址就是一种主机编址方式，给每个连接在 Internet 上的主机分配一个 32 位（bit，比特）地址，也称为网际协议地址。

按照 TCP/IP（Transport Control Protocol/Internet Protocol，传输控制协议/Internet 协议）

协议的规定，IP 地址用二进制来表示，每个 IP 地址长 32 位，位换算成字节就是 4 个字节。例如一个采用二进制形式的 IP 地址是 00001010000000000000000000000001，这么长的地址人们处理起来就会很费劲，为了方便使用，IP 地址经常被写成十进制的形式，中间使用符号“.”分为 4 个不同的十进制数，这样就可以用 XXX.XXX.XXX.XXX 的形式来表示，每组 XXX 代表小于等于 255 的十进制数，例如 192.168.38. 6。IP 地址的这种表示方法称为“点分十进制表示法”，这显然比二进制的 1 或 0 容易记忆。

IP 地址是如何划分的呢？在互联网中的每个接口有一个唯一的 IP 地址与其对应，该地址并不是平面形式的地址空间，而是具有一定的结构，一般情况下，IP 地址可以分为 5 大类，如图 1-1 所示。

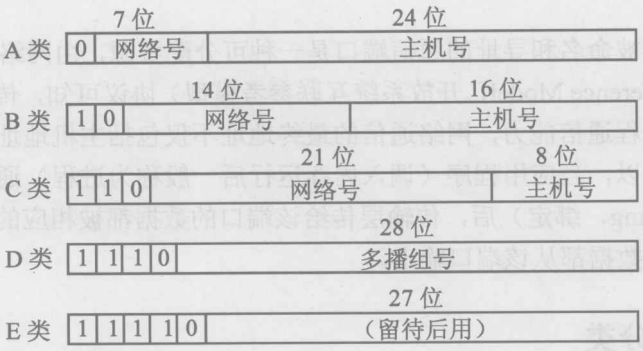


图 1-1　5 类 IP 地址

在 A 类中，第 1 段为网络位，后 3 段为主机位，其范围为 1～127，例如 127.255.255.255；在 B 类中，前两段是网络位，后两段为主机位，其范围为 128～191，例如 191.255.255.255；在 C 类中，前 3 段为网络位，后 1 段为主机位，其范围为 192～223，例如 223.255.255.255；D 类地址用于多播，也叫做组播地址，在互联网上不能作为接点地址使用，其范围为 224～239，例如 239.255.255.255；E 类地址用于科学研究，也不能在互联网上使用，其范围为 240～254。

注意：全 0 和全 1 的 IP 地址禁止使用，因为全 0 代表本网络，而全 1 是广播地址（在 CISCO 上可以使用全 0 地址）。一般情况下，常用的是 A、B、C 这 3 类地址。

1.2　黑客的专用通道：端口

随着网络技术的发展，原来物理上的端口（例如，鼠标、键盘、网卡、显卡等输入/输出接口）已不能满足网络通信的要求，而 TCP/IP 协议则被集成到了操作系统的内核中，这就相当于在操作系统中引入了一种新的输入/输出接口技术。因为在 TCP/IP 协议中引入了一种被称为 Socket 的应用程序接口技术，这就使得一台计算机可以通过软件方式与任何一台具有 Socket 接口的计算机进行通信。

1.2.1 端口的概念与作用

端口（port）可以认为是计算机与外界通讯交流的出口。其中硬件领域的端口又称接口，例如，USB 端口、串行端口等。软件领域的端口一般指网络中面向连接服务和无连接服务的通信协议端口，是一种抽象的软件结构，包括一些数据结构和 I/O（基本输入/输出）缓冲区。

端口是传输层的内容，是面向连接的，它们对应着网络上常见的一些服务。这些常见的服务可划分为使用 TCP 端口（面向连接，如打电话）和使用 UDP 端口（无连接，如写信）两种。

在网络中可以被命名和寻址的通信端口是一种可分配资源，由网络 OSI（Open System Interconnection Reference Model，开放系统互联参考模型）协议可知，传输层与网络层的区别是传输层提供进程通信能力，网络通信的最终地址不仅包括主机地址，还包括可描述进程的某种标识。所以，当应用程序（调入内存运行后一般称为进程）通过系统调用与某端口建立连接（Binding，绑定）后，传输层传给该端口的数据都被相应的进程所接收，相应进程发给传输层的数据都从该端口输出。

1.2.2 端口的分类

在网络技术中，端口大致有两种意思：一是物理意义上的商品，例如，集线器、交换机、路由器等用于连接其他网络设备的接口；二是逻辑意义上的端口，一般指 TCP/IP 协议中的端口，范围为 0～65535，例如，浏览网页服务的 80 端口，用于 FTP 服务的 21 端口等。

逻辑意义上的端口有多种分类标准，常见的分类标准有如下两种。

1. 按端口号分布划分

按端口号分布划分可以分为公认端口、注册端口以及动态和/或私有端口等。

- 公认端口

公认端口（Well Known Ports）也称为常用端口，端口号为 0～1023，它们紧密地绑定于一些特殊的服务。通常，这些端口的通信明确地表明了某种服务协议，不可再重新定义它的作用对象。例如，21 端口分配给 FTP 服务；23 号端口分配给 Telnet 服务专用；25 号端口分配全 SMTP（简单邮件传输协议）服务；80 端口是 HTTP 通信使用的；135 端口分配给 RPC（远程过程调用）服务等，通常不会被像木马这样的黑客程序利用。

- 注册端口

注册端口（Registered Ports）的端口号为 1024～49151，它们松散地绑定一些服务，也即有许多服务绑定于这些端口，这些端口同样用于许多其他目的，并且多数没有明确定义对象，不同的程序可以根据需要自己定义。记住这些常见程序端口，在木马程序的防护和查杀上非常有必要。

❑ 动态和/或私有端口

动态和/或私有端口（Dynamic and/or Private Ports）的端口号为 49152～65535，理论上不应该把常用服务分配在这些端口上，但实际上有些较为特殊的程序，特别是一些木马程序就非常喜欢使用这些端口，因为这些端口常常不会引起人们的注意，容易隐蔽。

2. 按协议类型划分

根据所提供的服务方式，端口又可分为 TCP 端口和 UDP 端口两种。一般直接与接收方进行的连接方式，大多是采用 TCP 协议；如果只是把信息放在网上发布出去而不去关心信息是否到达，也就是无连接方式，这种方式则大多采用 UDP 协议。

使用 TCP 协议的常见端口主要有如下几种。

❑ FTP

定义了文件传输协议，使用 21 端口。某计算机开通了 FTP 服务便启动了文件传输服务，下载文件和上传主页都要用到 FTP 服务。

❑ Telnet

一种用于远程登录的端口，用户可以以自己的身份远程连接到计算机上。通过这种端口可提供一种基于 DOS 模式的通信服务，例如支持纯字符界面 BBS 的服务器会将 23 端口打开，以对外提供服务。

❑ SMTP

现在很多邮件服务器都是使用这个简单邮件传送协议来发送邮件的。例如常见免费邮件服务中使用的就是此邮件服务端口，所以在电子邮件设置中经常会看到有 SMTP 端口设置栏，服务器开放的是 25 号端口。

❑ POP3

POP3 协议用于接收邮件，通常使用 110 端口。只要有相应使用 POP3 协议的程序（例如 Outlook 等），即可直接使用邮件程序收到邮件（例如使用 126 邮箱的用户就没有必要先进入 126 网站，再进入自己的邮箱来收信了。）

使用 UDP 协议的常见端口主要有如下几种。

❑ HTTP

这是用户使用最多的协议，也即超文本传输协议。当上网浏览网页时，就要在提供网页资源的计算机上打开 80 号端口以提供服务。通常的“WWW 服务”、“Web 服务器”等使用的就是这个端口。

❑ DNS

DNS 用于域名解析服务，这种服务在 Windows NT 系统中用得最多。Internet 上的每一台计算机都有一个网络地址与之对应，这个地址就是 IP 地址，它以纯数字的形式表示。但由于这种表示方法不便于记忆，于是就出现了域名，访问计算机时只需要知道域名即可，域名和 IP 地址之间的变换由 DNS 服务器来完成（DNS 用的是 53 号端口）。

❑ SNMP

简单网络管理协议，用来管理网络设备，使用 161 号端口。

❑ QQ

QQ 程序既提供服务又接收服务，使用的是无连接的协议，即 UDP 协议。QQ 服务器使用 8000 号端口侦听是否有信息到来，客户端使用 4000 号端口向外发送信息。

提示： 在计算机的 6 万多个端口中，通常把端口号为 1024 以内称为常用端口，这些常用端口所对应的服务通常情况下是固定的。

1.2.3 查看端口

为了查找目标主机上都开放了哪些端口，可以使用某些扫描工具对目标主机一定范围内的端口进行扫描。只有掌握目标主机上的端口开放情况，才能进一步对目标主机进行攻击。

在 Windows 2000/Server 2003/XP 系统中，可以使用 Netstat 命令查看端口。选择【开始】→【运行】命令，即可打开【运行】对话框并在其中运行 cmd 命令，如图 1-2 所示；或选择【开始】→【所有程序】→【附件】→【命令提示符】命令，即可打开【命令提示符】窗口。在命令提示符后输入“netstat -a -n”命令并运行之后，即可看到以数字形式显示的 TCP 和 UDP 连接的端口号及其状态，如图 1-3 所示。

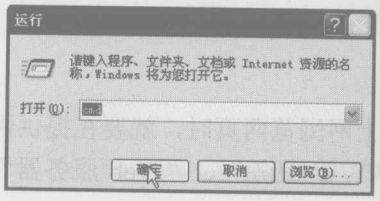


图 1-2　【运行】对话框

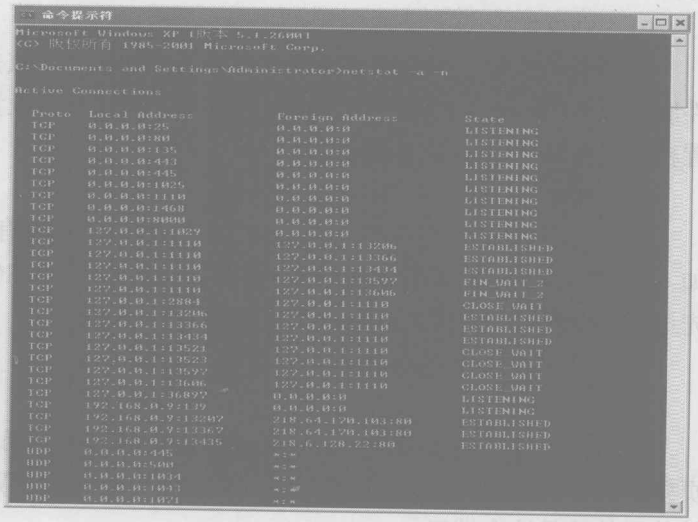


图 1-3　查看端口号状态

如果攻击者使用扫描工具对目标主机进行扫描，即可获取目标计算机打开端口的情况，并了解目标计算机提供了哪些服务。根据这些信息，攻击者就可以对目标主机有一个初步的了解。

如果在管理员不知情的情况下打开了太多端口，则可能出现两种情况：一种是提供的服务管理者没有注意到，例如安装 IIS 服务时，软件就会自动地增加很多服务；另一种是服务器被攻击者植入了木马程序，通过特殊的端口进行通信。这两种情况都比较危险，管理员不了解服务器提供的服务，就会减小系统的安全系数。