不怕是新手 轻松学得会

全新互动多媒体学习模式

新手学黑客攻防

神龙工作室 编著

易学易用

看得懂： 按照初学者接受知识的难易程度，由浅入深地组织内容

学得会： “语言通俗易懂+实例精彩丰富+初学者常见问题解答”的完美结合，帮助您轻松学会黑客攻防的方法

用得巧： 与读者的工作和生活紧密结合，学有所用

超值光盘

视频教学： 3个小时情景•互动式多媒体视频教学

超值奉送： 200个黑客攻防常见问题解答

人民邮电出版社
POSTS & TELECOM PRESS

新手学黑客攻防

神龙工作室 编著

人民邮电出版社
北京

图书在版编目（CIP）数据

新手学黑客攻防 / 神龙工作室编著. —北京：人民邮电出版社，2009.2（2009.5 重印）
ISBN 978-7-115-19512-8

Ⅰ. 新… Ⅱ. 神… 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204822号

内 容 提 要

本书是指导初学者快速掌握黑客攻防的入门书籍。书中详细地介绍了初学者必须掌握的黑客攻防的基础知识和方法，并对初学者在使用攻防工具时经常遇到的问题进行了专家级的指导，以免初学者在起步的过程中走弯路。本书分为 4 篇，共 14 章。第 1 篇（第 1 章）主要介绍黑客的基础知识，包括 IP 地址、端口、黑客常用的命令及攻击方式，第 2 篇（第 2~3 章）主要介绍黑客如何运用检测工具检测并扫描电脑等内容，第 3 篇（第 4~11 章）主要介绍一些典型的黑客攻防技术，第 4 篇（第 12~14 章）主要介绍防范黑客攻击的方法和技巧。

本书附带一张情景、互动式多媒体教学光盘，可以帮助读者快速掌握黑客攻防的知识和方法。同时光盘中还赠送一本包含 200 个黑客攻防常见问题解答的电子图书，大大地扩充了本书的知识范围。

本书主要面向使用电脑的初级用户，适合广大电脑爱好者以及各行各业需要学习电脑防御技术的人员使用，同时也可以作为学习黑客攻防技术的培训教材或者辅导教材。

新手学黑客攻防

◆ 编　　著　神龙工作室
责任编辑　魏雪萍

◆ 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
北京铭成印刷有限公司印刷

◆ 开本：787×1092　1/16
印张：16.25
字数：413 千字　　2009 年 2 月第 1 版
印数：8 001 – 11 000 册　　2009 年 5 月北京第 2 次印刷

ISBN 978-7-115-19512-8/TP

定价：29.80 元（附光盘）

读者服务热线：(010)67132692　印装质量热线：(010)67129223
反盗版热线：(010)67171154

Preface 前言

黑客很神秘吗?

不神秘!

学习黑客攻防技术难吗?

不难!

阅读本书能掌握防范黑客攻击的技术吗?

能!

为什么要阅读本书

网络在人们的生活、学习和工作等许多方面都起着举足轻重的作用，人们越来越离不开网络，与此同时，网络的安全问题也随之出现。对于普通人而言，掌握一定的黑客攻防技术不仅能够帮助您保护电脑中资料的安全，而且可以帮助您更好地维护电脑，保障其安全、稳定地运行，以给您的工作和生活带来极大的便利。

作为学习黑客攻防技术的新手，您是否也曾为不了解黑客常用命令而发愁，您是否也曾为使用黑客常用工具而苦恼，您是否也曾为保障密码安全而冥思苦想，您是否也曾为防范病毒和木马的攻击而力不从心……如果您掌握了黑客攻击、防范的技能和通用方法，多思考，勤动手，那么这些问题都会迎刃而解。基于这个出发点，我们组织了具有多年维护经验的电脑防御专家，为爱好学习黑客攻防技术的初学者编写了这本“入门”书籍。通过阅读本书，您也可以游刃有余地处理各种电脑安全问题，轻松自如地管理电脑。

本书是否适合您

如果您是第一次接触黑客知识，本书将从初学者的角度出发，一步一步地引导您掌握黑客的基础知识及常用命令；如果您还不知道黑客常用的攻击、防范技术，本书将以实例的形式，让您在边学边做的过程中通晓各种黑客常用工具的使用及防范技巧；如果您对理论性的黑客攻防书籍感到费解，本书将以实例图解、视频辅助的教学方式让您轻松掌握病毒及木马的防范技巧。

阅读本书能学到什么

了解黑客常用工具的使用方法

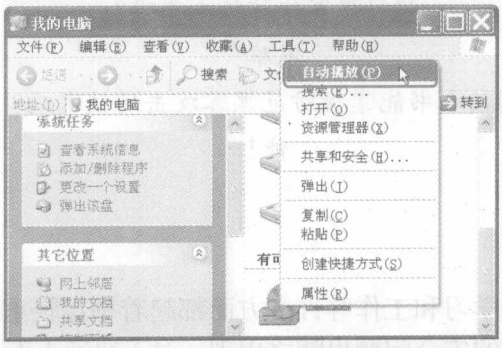
掌握典型的黑客攻防技巧

掌握电脑安全策略设置方法

掌握常用的防护软件的使用方法

CD-ROM 配套光盘使用说明

1 将光盘印有文字的一面朝上放入光驱中，几秒钟后光盘就会自动运行。若光盘没有自动运行，可以打开【我的电脑】窗口，然后在光盘图标上单击鼠标右键，从弹出的快捷菜单中选择【自动播放】菜单项，光盘就会运行。



2 首先会播放一段片头动画，接着播放光盘中的人物介绍（单击鼠标左键可以跳过该环节），稍后会进入光盘的主界面，此时可以看到光盘中包含的各个章节目录。

3 将鼠标指针移到目录按钮上单击左键，弹出对应的下一级子目录，然后单击某个子目录按钮即可进入光盘播放界面，并自动播放该节的内容。

Contents 目录

第1篇 黑客基础

第2篇 黑客技术

第3篇 典型攻防

第4篇 系统安全配置

具体内容参见本书附带光盘

常见问题解答目录

常见问题解答200例

系统设置与账户管理常见技巧

办公应用中常见技巧

漏洞与病毒常见技巧

网络常见技巧

第 1 篇

黑客基础

黑客，在人们的印象中是一个神秘的词汇。人们都认为黑客具有高超的电脑和网络方面的技术，可以通过网络完成一些一般人完成不了的电脑操作。但是，恐怕很少有人知道要成为一名黑客需要掌握一些最基本的知识。本篇介绍这些基本知识，包括基本的网络知识，常用的网络命令和一些 DOS 命令。

新手

第 1 章
拨云见日——了解黑客

Chapter 1

小龙：小月，我经常听到“黑客”这个词，到底什么是黑客？黑客很厉害吗？

小月：呵呵，黑客其实和我们一样，不过他们可是电脑和网络方面的高手。

小龙：那我也能成为“黑客”吗？

小月：当然可以了！只要你好好学习电脑和网络方面的知识一定可以。

小龙：是吗？太好了，你快教教我吧！

小月：好的，我们就先从了解黑客开始吧。

要点导航

- 什么是黑客
- IP 地址及端口知识
- 黑客的常用命令
- 黑客常用的攻击方式

1.1 什么是黑客

一提起黑客，人们总会将他们和破坏网络安全、盗取网络密码等联系在一起，感到他们非常神秘。那么，黑客到底是一群什么样的人？他们从事什么活动？本节将揭开黑客的神秘面纱。

黑客，又称骇客，来源于英文单词 hacker。其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。这些人往往都掌握有非凡的电脑和网络知识，除了无法通过正当的手段物理性地破坏他人的电脑和帮助他人重装操作系统外，其他的几乎绝大部分的电脑操作他们都可以通过网络做到，例如监视他人计算机、入侵网站服务器替换该网站的主页、攻击他人电脑、盗取电脑中的文件等。

黑客刚出现时，其活动的理由一般都很简单，大部分人只是为了炫耀一下自己的电脑技巧，或者开一些善意的玩笑。现在，一些人会使用简单的工具对一些疏于防范的电脑进行攻击并破坏，这已经不属于黑客的范畴了，而是犯罪活动。在日常生活中，许多电脑故障都是出自黑客之手，例如某网站无法访问等。

现在黑客技术已经被越来越多的人掌握，其发展也日益加快。目前，世界上有很多黑客网站，这些网站会介绍一些常用的攻击方法和系统的一些漏洞，并免费提供一些常用的攻击软件供网友下载和使用，这样普通用户掌握后也可以攻击其他的电脑。但是黑客技术同时又是一把双刃剑，了解了常用的黑客技术，就可以更好地保护自己的电脑不受恶意攻击。

在网络发展初期，网络方面的立法还不够健全，黑客在法律的漏洞下可以在网络上为所欲为。现在，各国法律的完善速度虽然还远远落后于网络的发展速度，但在现有法律的打击下，黑客活动已经转入地下，其攻击的隐蔽性也更强了，使得当前的法律和技术还缺乏针对网络犯罪的有效的反击和跟踪手段。目前，无规范的黑客活动已成为网络安全的重要威胁。

实际上，非法攻击电脑和站点已经不属于黑客行为。黑客群体有自己的处事态度：解决问题并创造新东西，相信自由并自愿地相互帮助。他们也有自己的精神（黑客精神）。

(1) 这世界充满待解决的迷人问题。

(2) 没有任何人必须一再地解决同一个问题。

(3) 无聊而单调的工作是有害的。

(4) 态度并不等效于能力。

(5) 自由才好。

黑客们也需要遵守一些默认的规则，这些规则就是人们所说的黑客守则。

(1) 不恶意破坏任何系统，这样只会带来麻烦，恶意破坏他人的软体将导致法律责任。

(2) 不修改任何的系统档，如果为了要进入系统而修改它，则在达到目的后将它改回原状。

(3) 不要轻易地将要 Hack 的站点告诉不信任的朋友。

(4) 不要在 BBS 上谈论任何黑客行为。

(5) 在 Post 文章的时候不要使用真名。

(6) 正在入侵的时候，不要随意离开电脑。

(7) 不要侵入或破坏政府机关的主机。

(8) 不要在电话中谈论 Hack 的任何事情。

(9) 将笔记放在安全的地方。

(10) 想要成为黑客就要真正的 hacking，读遍所有有关系统安全或系统漏洞的文件。

(11) 已侵入电脑中的账号不得清除或涂改。

(12) 不得修改系统档案，如果为了隐藏自己的侵入而做的修改则不在此限，但仍须维持原

来系统的安全性，不得因得到系统的控制权而将门户大开。

⑬ 不将已破解的账号分享于朋友。

1.2 IP地址及端口知识

在现实生活中，每个人都有一个名字，一个人也可能有多个名字，多个人也可能使用同一个名字。Internet 中的网络主机也是这样，可以使用域名来为其命名。因此在网络上能够真正标识主机的就是 IP 地址。在网络连通的情况下，只要利用域名或者 IP 地址都是可以找到目的主机的，因此如果想要攻击某个网络主机，首先要确定该目标的域名或者 IP 地址。

一台电脑可能同时运行几个不同的网络服务程序，那么电脑是怎么分辨出网络上的数据是对应哪个程序的呢？这就需要通过端口来区分，不同的程序启用不同的端口，这样电脑就可以区别。

1.2.1 IP 地址

IP 是英文 Internet Protocol 的缩写，意思是“网络之间互连的协议”，也就是为电脑网络相互连接进行通信而设计的协议。在因特网中，它是能使连接到网上的所有电脑网络实现相互通信的一套规则，规定了电脑在因特网上进行通信时应当遵守的规则。当我们把整个互联网看做一个单一的网络时，IP 地址就是给每个连接在网络上的主机（或路由器）分配的一个全球唯一的 32bit（IPv4 是 32bit，IPv6 是 128bit；本书在以后提到 IP 协议除非特别声明，否则均指 IPv4。bit：比特，一位二进制数就是 1 比特）的标识符。

IP 地址的结构使我们可以在互联网上很方便地进行寻址。IP 地址由因特网名字与号码指派公司 ICANN（Internet Corporation for Assigned Names and Numbers）进行分配。

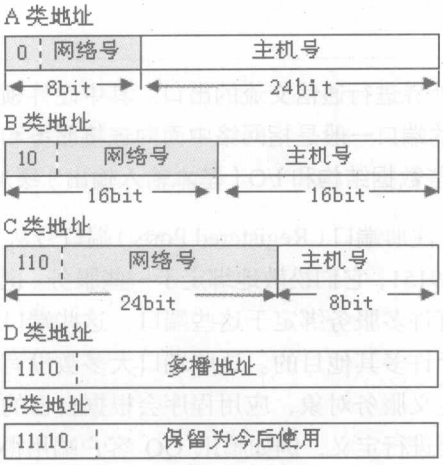
1. IP 地址的表示法

按照 TCP/IP（Transport Control Protocol/Internet Protocol，传输控制协议/网际协议）的规定，IP 地址用二进制来表示，每个 IP 地址长 32bit，也就是 4 个字节。例如，一个采用二进制形式记录的 IP 地址是“11000000000010100000101010000001”，这么长的一串字符人们处理起来会很不方便。为了便于人们使用，IP 地址的每个字节经常被记录成十进制形式，字节之间用“.”分开，即 XXX.XXX.XXX.XXX 的形式，每组 XXX 代表小于等于 255 的十进制正整数，例如上面的地址就可以表示为：192.10.10.193，IP 地址的这种表示法称为“点分十进制表示法”，显然这种表示法比用二进制表示容易记忆。

也许有人会认为一台主机只能有一个 IP 地址，这种观点是错误的，事实上，一台主机可以有多个 IP 地址。另外我们也可以通过特定的技术使多台主机共用一个 IP 地址，这样，这些主机在用户看来就像一台主机一样。

2. IP 地址的分类

IP 地址结构采用的是非平面的分层架构的地址空间。在互联网早期，IP 地址被分为了 5 大类，如下图所示。



用点分十进制表示法表示，A 类地址则以第 1 个字节为网络号，其中第 1 位为 0，其范围为 1.0.0.1 ~ 126.255.255.254；B 类地址以前两个字节为网络号，其中第 1 个字节的前两位必须是 10，其范围为 128.0.0.1 ~ 191.255.255.254；C 类地址以前 3 个字节为网络号，其中第 1 个字节的前 3 位必须是 110，其范围为 192.0.0.1 ~ 223.255.255.254；D 类地址不分网络号和主机号，它的第 1 个字节的前 4 位固定为 1110，其范围为 224.0.0.1 ~ 239.255.255.254。D 类地址用于多播通信（一对多通信），主要留给因特网体系结构委员会 IAB（Internet Architecture Board）使用。E 类地址不分网络号和主机号，它的第 1 个字节的前 5 位固定为 11110，其范围为 240.0.0.1 ~ 255.255.255.254，E 类地址保留为以后使用。也许有人已经发现在上面几类地址的划分中没有 127.0.0.1 ~ 127.255.255.254 地址段，这是因为这一地址段保留作为本地软件环回测试本主机之用，例如 127.0.0.1 就是指本机。另外，A 类地址中的地址段 10.0.0.0 ~ 10.255.255.255，B 类地址中的地址段 172.16.0.0 ~ 172.31.255.255 和 C 类地址中的地址段 192.168.0.0 ~ 192.168.255.255 等作为私有地址，不能用在互联网上，而只能用于局域网。

需要指出的是：由于 IPv4 地址的枯竭，IPv6 技术尚不成熟，为了减缓 IP 地址的枯竭速度，近年来已经广泛使用无分类的 IP 地址，A 类、B 类、C 类地址的区分已成为历史。本书限于篇幅的原因就不介绍无分类 IP 地址了，有兴趣的读者可以自己查阅资料。

3. IPv6 地址简介

随着互联网的发展，网络上的主机越来越多，IP 地址渐渐枯竭，虽然使用无分类 IP 地址减缓了它的枯竭速度，但并不能完全解决这个问题。为了彻底解决这个问题，人们开发出了具有更大地址空间的新版本 IP 协议，即 IPv6。下面简单介绍一下 IPv6 的 IP 地址。IPv6 将 IP 地址从 32bit 扩展为 128bit，地址空间增大了 296 倍，这样大的空间在可预见的未来是不会用完的，因此 IPv6 号称“可以给地球上的第一粒沙子分配一个 IP 地址”。由于 IPv6 使用 128 位的地址，所以 IPv4 使用的点分十进制表示法就不够方便了。例如，下面是一个用点分十进制表示的 IPv6 地址：104.230.140.100.255.255.255.255.0.0.17. 128.150.10.255.255。为了使地址再简单一些，它使用冒号十六进制表示法，把每两个字节（16bit）的值用十六进制表示，各值之间用冒号分隔，如上面的地址就可以表示为 68E6:8C64:FFFF:FFFF:0:1180:960A:FFFF。冒号十六进制表示法可以采用零压缩技术，即一连串连续的 0 可以用一对冒号替代，如 FF05:0:0:0:0:0:0:B3 可以表示为 FF05::B3。为了保证零压缩有一个唯一的解释，IPv6 规定在任一个地址中只能使用一次零压缩。另外，冒号十六进制表示法还可以结合点分十进制表示法的后缀，再使用零压缩技术就可以方便地实现 IPv4 和 IPv6 的互相转换。例如一个 IPv4 地址 128.0.0.1 转换为 IPv6 地址就可以记为 0:0:0:0:0:0:128.0.0.1，再使用零压缩后就可以表示为：128.0.0.1。

事实上，有关 IP 地址的知识是相当多的，受本书篇幅所限，这里不再介绍，有兴趣的读者可以自己查阅资料。

1.2.2 端口

“端口”是英文 port 的译义，可以认为是电脑与外界进行通信交流的出口。其中硬件领域的端口又称接口，如 USB 端口、串行端口等。软件领域的端口一般是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。

在网络技术中，端口（Port）的含义有多种。集线器、交换机、路由器的端口指的是连接其他网络设备的接口，如 RJ-45 端口、Serial 端口等。我们这里所指的端口不是指物理意义上的端口，而是特指 TCP/IP 协议中的端口，是逻辑意义上的端口。

端口是用来解决主机应该把接收到的数据包传送给众多同时运行的进程中的哪一个的问题的。例如 http 协议使用 80 号端口，FTP 协议使用 21 号端口，这样通过不同的端口，电脑同时运行的不同进程就可以互不干扰地进行通信了。通常来说，一台电脑一般有 65535 个端口，而常用的端口也就几十个，由此可见，我们还有大量的端口没有使用。这样，黑客程序就可以采用某种方法，打开我们没有使用的端口，从而对电脑进行控制。

1. 端口的分类

这 65535 个端口按不同的分类标准可以分为多类，其中最常用的分类标准有以下两种。

按端口号分，端口可以分为三大类，分别是“公认端口”、“注册端口”和“动态和/或私有端口”。

公认端口

公认端口（Well Known Ports）的端口号从 0 到 1023，它们紧密绑定于一些服务。通常这些端口的通信明确表明了某种服务的协议，这种端口不可再重新定义它的作用对象。例如 80 端口是 HTTP 通信所使用，21 端口是 FTP 服务所使用，23 端口是 Telnet 服务所使用，SMTP（简单邮件传输协议）使用 25 号端口，等等。

注册端口

注册端口（Registered Ports）端口号从 1024 到 49151，它们松散地绑定于一些服务。也就是说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。这些端口大多数没有明确的定义服务对象，应用程序会根据自己的实际需要进行定义，例如腾讯 QQ 客户端用得就是 4000 端口。需要指出的是：这些端口也是木马程序的常用端口，是防护和查杀木马程序必须要检查的端口。

动态和/或私有端口

动态和/或私有端口（Dynamic and/or Private Ports）端口号从 49152 到 65535。理论上不应为服务分配这些端口，但实际上一些较为特殊的程序，特别是一些木马程序就喜欢使用这些端口，因为这些端口通常不被人们注意，容易隐蔽。事实上，机器通常从 1024 起分配动态端口，但也有例外：SUN 的 RPC 端口就是从 32768 开始。

网络上常用的通信有两种，分别是面向连接（TCP，传输控制协议）和无连接（UDP 协议，用户数据报协议）。电脑端口也可以分为这两类，即“TCP 端口”和“UDP 端口”。面向连接通信要经过 3 个阶段：数据传数前，先建立连接，连接建立后再传输数据，数据传送完后释放连接。面向连接通信，可确保数据传送的次序和传输的可靠性，采用的是 TCP（传输控制协议）。无连接通信只有传输数据阶段，消除了除数据通信外的其他开销。只要发送实体是活跃的，无须接收实体也是活跃的。它的优点是灵活方便、迅速，特别适合于传送少量零星的报文，但无连接服务不能防止报文的丢失、重复或失序，它采用的是 UDP 协议（用户数