
HZ BOOKS
华章科技
DVD
学电脑从入门到精通
THE SECRETS OF BEING AN EXPERT
IN COMPUTER FROM A BEGINNER
黑客攻防
从入门到精通
恒盛杰资讯 编著
多媒体视频+技巧+案例的学习模式
赠送重点、难点及案例多媒体视频讲解
赠送《黑客攻防秘笈》电子书
机械工业出版社
China Machine Press

学电脑从入门到精通

黑客攻防
从入门到精通

恒盛杰资讯　编著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

黑客攻防从入门到精通 / 恒盛杰资讯编著 . —北京：机械工业出版社，2013.3
（学电脑从入门到精通）
ISBN 978-7-111-41765-1

Ⅰ. 黑… Ⅱ. 恒… 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（2013）第 047279 号

本书全面且详细地介绍了黑客攻防的基础知识，主要包括黑客攻防前的准备工作、扫描与嗅探攻防、Windows 系统漏洞攻防、密码攻防、病毒攻防、木马攻防等内容。虽然书中介绍了黑客入侵攻击目标计算机的一些相关操作，但是这不是本书的重点，本书的重点在于介绍如何采取有效的防范措施来防御黑客入侵攻击自己的计算机。

本书按照由易到难、循序渐进的顺序安排知识点。本书图文并茂，讲解深浅适宜，叙述条理清楚，通过阅读本书，读者不仅能了解黑客入侵攻击的原理和使用工具，而且还能掌握防御入侵攻击的相关操作。本书配有多媒体教学光盘，光盘中提供了相关的视频教学演示。

本书适用于计算机初学者，也适用于计算机维护人员、IT 从业人员以及对黑客攻防与网络安全维护感兴趣的计算机中级用户，同时也可作为各种计算机培训班的辅导用书。

机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码 100037）
责任编辑：陈佳媛
北京瑞德印刷有限公司印刷
2013 年 4 月第 1 版第 1 次印刷
185mm × 260mm • 22 印张
标准书号：ISBN 978-7-111-41765-1
ISBN 978-7-89433-831-0（光盘）
定 价：49.00 元（附光盘）

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991 88361066 投稿热线：（010）88379604
购书热线：（010）68326294 88379649 68995259 读者信箱：hzjsj@hzbook.com

前言

在 Internet 中，黑客通常都是一类拥有高超计算机技术的人，他们甚至不需要亲自接触用户的计算机，就可以偷窥其中的账户、密码等信息，甚至破坏其操作系统。随着越来越多的金融贸易要通过 Internet 来实现，防御黑客入侵已成为至关重要的工作。作者特为此编写了本书。

主要内容

本书包括 17 章，第 1 章介绍了黑客的基础知识，包括 IP 地址、端口、系统进程以及 DOS 命令等内容；第 2 章介绍了黑客攻防前的准备工作，包括安装 VMware 和虚拟操作系统，认识黑客常用的入侵工具、入侵方法以及防护策略等内容；第 3 章介绍了扫描与嗅探攻防的知识，包括搜索目标计算机的 IP 地址、扫描其端口以及嗅探网络中的数据包等内容；第 4 章介绍了 Windows 系统漏洞攻防的相关知识，包括认识、检测和修复 Windows 系统漏洞等内容；第 5 章介绍了密码攻防的相关知识，包括解除系统中的密码、破解文件密码以及防范密码被轻易破解等内容；第 6 ~ 7 章介绍了病毒、木马攻防相关知识，包括认识病毒木马、制作病毒木马以及防范病毒木马等内容；第 8 ~ 10 章介绍了后门技术、局域网和远程控制攻防的相关知识，包括认识后门、制作后门、清除日志信息、防御局域网中的攻击类型以及常见的远程入侵方式等内容；第 11 ~ 13 章介绍了 QQ、E-Mail 与 IE 浏览器和网站攻防的相关知识，包括盗取 QQ 密码和远程攻击 QQ、保护 QQ 密码和聊天记录、攻击 IE 浏览器和电子邮箱、DoS 攻击、DDoS 攻击等内容；第 14 ~ 16 章介绍了防范流氓与间谍软件、计算机安全防护以及系统与数据的备份与恢复的相关知识，包括清除流氓软件与间谍软件、系统 \ 注册表 \ 组策略的安全设置以及系统的备份与还原等内容；第 17 章

介绍了网络支付工具安全的相关知识，包括防御黑客入侵支付宝账户、网上银行以及财付通等内容。

本书特色

简单易懂——本书为了能适用于初次接触黑客攻防技术的用户，将黑客入侵攻击演示以及防御黑客入侵的操作以图文结合的形式进行介绍，使读者可以轻松地掌握有关黑客入侵目标计算机和防御黑客入侵计算机的基础知识。

内容丰富——本书中添加了“提示”版块，既包括为读者答疑解惑的纯文字内容，又包括帮助读者提高动手能力的图文解析内容，帮助读者答疑解惑。

读者对象

本书内容详细，讲解具体，充分融入了作者的实际使用经验和操作心得，可以作为个人学习和了解黑客攻防的参考书籍。

希望本书能对广大读者朋友有所帮助。由于作者水平有限，在编写本书的过程中难免会存在疏漏之处，恳请广大读者批评指正，可登录 www.epubhome.com 网站提出宝贵意见。

作者

2013 年 2 月

目录

第14章 防范流氓与间谍软件 / 252

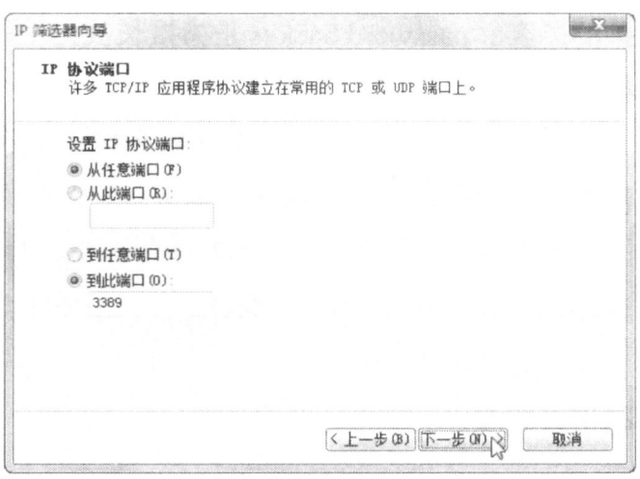
第15章 计算机安全防护设置 / 261

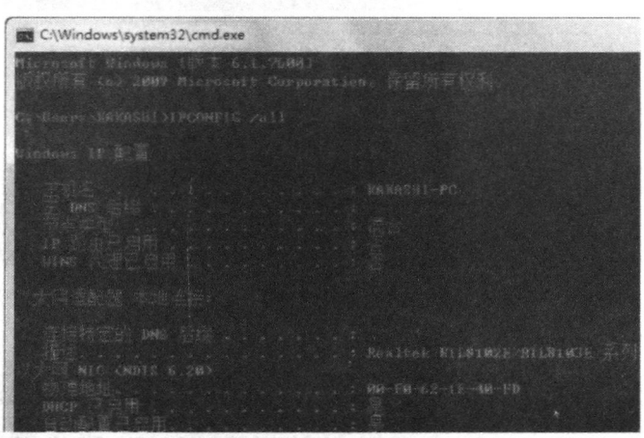
第16章 系统与数据的备份与恢复 / 290

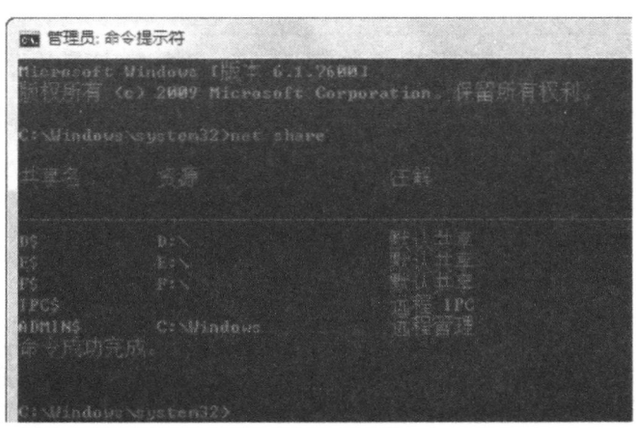
第17章 加强网络支付工具的安全 / 317

第1章 从零开始认识黑客

如今，Internet 在人们的生活、工作和学习中起着十分重要的作用。但是，随之而来的却是 Internet 的安全问题越来越突出。在 Internet 中，有一类人，他们掌握高超的计算机技术，可能他们会维护 Internet 的安全，可能他们会破坏 Internet 的安全，这类人就是黑客——一个让绝大部分网络用户敬畏的人群。







知识要点

- 认识黑客
- 黑客的专用通道——端口
- 认识黑客常用的 DOS 命令
- 黑客的定位目标——IP 地址
- 黑客藏匿的首选地——系统进程

1.1 认识黑客

黑客是一类掌握超高计算机技术的人群。凭借着掌握的知识，他们既可以从事保护计算机和网络安全的工作，又可以选择入侵他人的计算机或者破坏网络，对于黑客而言，他们所做的事情总是带有一定的目的，也许是为了炫耀，也许是为了报复。

1.1.1 区别黑客与骇客

黑客的原意是指那些精通操作系统和网络技术，并利用其专业编制新程序的人。黑客所做的不是恶意破坏，他们是一群纵横于网络上的技术人员，热衷于科技探索、计算机科学研究。在黑客圈中，Hack 一词带有正面的意义，例如 system hack 是指熟悉操作系统的设计与维护的黑客；password hacker 是指擅长找出使用者密码的黑客；computer hacker 则是指通晓计算机，可让计算机乖乖听话的黑客。

而骇客则不一样，骇客是指利用所掌握的计算机技术，从事恶意破解商业软件、恶意入侵别人的网站或计算机等事务的人。

总的来说，黑客是一类主要负责维护计算机和网络的安全的人员，而骇客则是入侵他人计算机或者网络的人员。其实黑客与骇客本质上都是相同的，即闯入计算机系统 / 软件者。黑客和骇客并没有一个十分明显的界限，但随着两者含义越来越模糊，因此造成了黑客一词越来越接近骇客。

提示：认识红客

红客是英文单词 Honker 的中文音译，它代表着一种精神，即热爱祖国、坚持正义和开拓进取的精神。因此只要具备这种精神并热衷于计算机技术的人都可以成为 Honker。Honker 是 Hacker 中的一部分人，这部分人以维护国家利益为己任，不利用掌握的计算机和网络技术入侵自己国家的计算机或服务器。他们维护正义，为国争光。

1.1.2 成为黑客必须掌握的知识

用户若想成为黑客，并不是一朝一夕的事情，需要掌握大量的计算机专业知识和技术，如果只是掌握了基础的 DOS 命令和一两款远程控制工具是算不上黑客的。成为黑客必须掌握的知识包括：一定的英文水平、理解常用的黑客术语和网络安全术语、熟练使用常用 DOS 命令和黑客工具，以及掌握主流的编程语言以及脚本语言。

1. 一定的英文水平

黑客学习的计算机知识虽然主要来源于国内，但是却经常需要参考国外的相关资料和教程，而国外的资料和教程大多数为英文版本，因此就需要具有一定的英文水平，以确保能够看

懂国外的一些参考资料。

2. 理解常用的黑客术语和网络安全术语

在常见的黑客论坛中，经常会看到肉鸡、挂马和后门等词语，这些词语可以统称为黑客术语，如果不理解这些词语，则在与其他黑客交流技术或经验时就会有障碍。除了掌握相关的黑客术语之外，作为黑客，还需要掌握 TCP / IP 协议、ARP 协议等网络安全术语。

3. 熟练使用常用DOS命令和黑客工具

常用 DOS 命令是指在 DOS 环境下使用的一些命令，主要包括 Ping、netstat 以及 net 命令等。利用这些命令可以实现对应不同的功能，如，利用使用 Ping 命令可以获取目标计算机的 IP 地址以及主机名。而黑客工具则是指用来远程入侵或者查看是否存在漏洞的工具，例如使用 X-Scan 可以查看目标计算机是否存在漏洞，利用 EXE 捆绑器可以制作带木马的其他应用程序。

4. 掌握主流的编程语言以及脚本语言

从 Internet 中获取的黑客工具通常是其他黑客利用指定类别的编程语言（C++、Java 等）制作的，如果想要成为一名黑客高手，仅仅使用别人制作的工具是不够的，需要具有创新精神，通过掌握主流的 C++、Java 等编程语言来编制属于自己的黑客工具。同时还需要掌握 JavaScript，VBScript 等脚本语言，用于自己编写脚本，实现脚本入侵。

提示：认识黑客攻击的目的

黑客攻击目标计算机或服务器的目的主要有 3 个，分别是盗取账户密码、恶作剧以及炫耀高超的计算机技术，其中盗取账户密码属于违法的行为，用户一定不要使用本书介绍的黑客工具去入侵他人的计算机。

1.2 黑客的定位目标——IP 地址

IP 是 Internet Protocol 的简称，中文简称为“网协”，它是为计算机网络相互连接进行通信而设计的协议。无论任何操作系统，只要遵守 IP 协议就可以与 Internet 互联互通。而 IP 地址则是为了识别 Internet 或局域网中的电脑所产生的 32bit（bit 的中文名称是位，音译为比特）地址。下面就介绍什么是 IP 地址以及 IP 地址的分类。

1.2.1 认识 IP 地址

IP 地址其实就与现实生活中的住址一样，如果要将信件寄送给指定的好友，就必须知道该好友的住址，这样才能确保邮递员能够准确地将信件送到好友手中。在 Internet 中，计算机之间的通信就类似于现实生活中用户之间的通信，若想将信息发送给指定的计算机，就必须知

道目标计算机的 IP 地址。

IP 地址默认是利用二进制来表示的，目前的 IP 地址的长度为 32bit，例如采用二进制形式的 IP 地址是 11000000101010000000000100100101，这么长的 IP 地址处理起来会非常麻烦。因此为了方便使用，IP 地址经常被记为十进制形式的数字，分为 4 段，每段包括 8 位，并且在中间使用句点符号“.”隔开，这样上面的 IP 地址可以写成 192.168.1.32。这种记法叫做“点分十进制表示法”，与一长串的 1 和 0 相比，利用点分十进制表示法表示的 IP 地址更容易被记住。

1.2.2 IP 地址的分类

在 Internet 中，每个 IP 地址都包括两个标识码（ID），它们分别是网络标识码和主机标识码。网络 ID 能够告诉用户计算机所处的特定网络，而主机 ID 则用来区分该网络中的多台计算机。

根据 IP 地址中网络 ID 与主机 ID 表示的不同数据段，可以将 IP 地址划分为 A、B、C、D 和 E 类。这 5 类 IP 地址的定义方式如表 1-1 所示。

表 1-1 IP 地址的分类及定义

地址类别	定　义
A 类	第 1 段为网络地址，第 2 ～ 4 段为主机地址。网络 ID 的第 1 位必须是 0，因此该类 IP 地址中网络 ID 的长度为 8 位，主机 ID 的长度为 24 位，该类 IP 地址范围为 1.0.0.1 ～ 126.255.255.254，其子网掩码为 255.0.0.0
B 类	第 1 ～ 2 段为网络地址，第 3 ～ 4 段为主机地址。网络地址的前 2 位必须是 10，因此该类 IP 地址中网络 ID 的长度为 16 位，主机 ID 的长度为 16 位，该类 IP 地址范围为 128.1.0.1 ～ 191.254.255.254，其子网掩码为 255.255.0.0
C 类	第 1 ～ 3 段为网络地址，第 4 段为主机地址。网络地址的前 3 位必须是 110，因此该类 IP 地址中网络 ID 的长度为 24 位，主机 ID 的长度为 8 位，该类 IP 地址范围为 192.0.1.1 ～ 223.255.254.254，其子网掩码为 255.255.255.0
D 类	该类 IP 地址的第一个字节以 1110 开始，它是一个专门保留的地址，并不指向特定的网络。目前这类地址被用在多点广播（Multicast）中，其地址范围 224.0.0.1 ～ 239.255.255.254
E 类	该类 IP 地址以 11110 开始，为将来使用保留

除了以上介绍的 5 种 IP 地址以外，还有全 0 和全 1 的 IP 地址，其中全 0 的 IP 地址（0.0.0.0）是指当前网络，全 1 的 IP 地址（255.255.255.255）是广播地址（现在 CISCO 上可以使用全 0 地址）。

提示：认识 IPv4 地址与 IPv6 地址

IPv 是 Internet Protocol version 的简称，中文译为“网际协议版本”，目前 Internet 中常用的网际协议版本有 IPv4 和 IPv6 两个。随着 Internet 中电脑数量越来越多，IPv4 采用 32bit 地址长度，只能容纳大约 43 亿台电脑，而 IPv6 采用了 128bit 地址长度，几乎可以不受限制地提供 IP 地址。按保守方法估算，IPv6 可以在全球每平方米的面积上，除了能够提供现有的地址数量之外，还可以增加大约 1000 个地址。