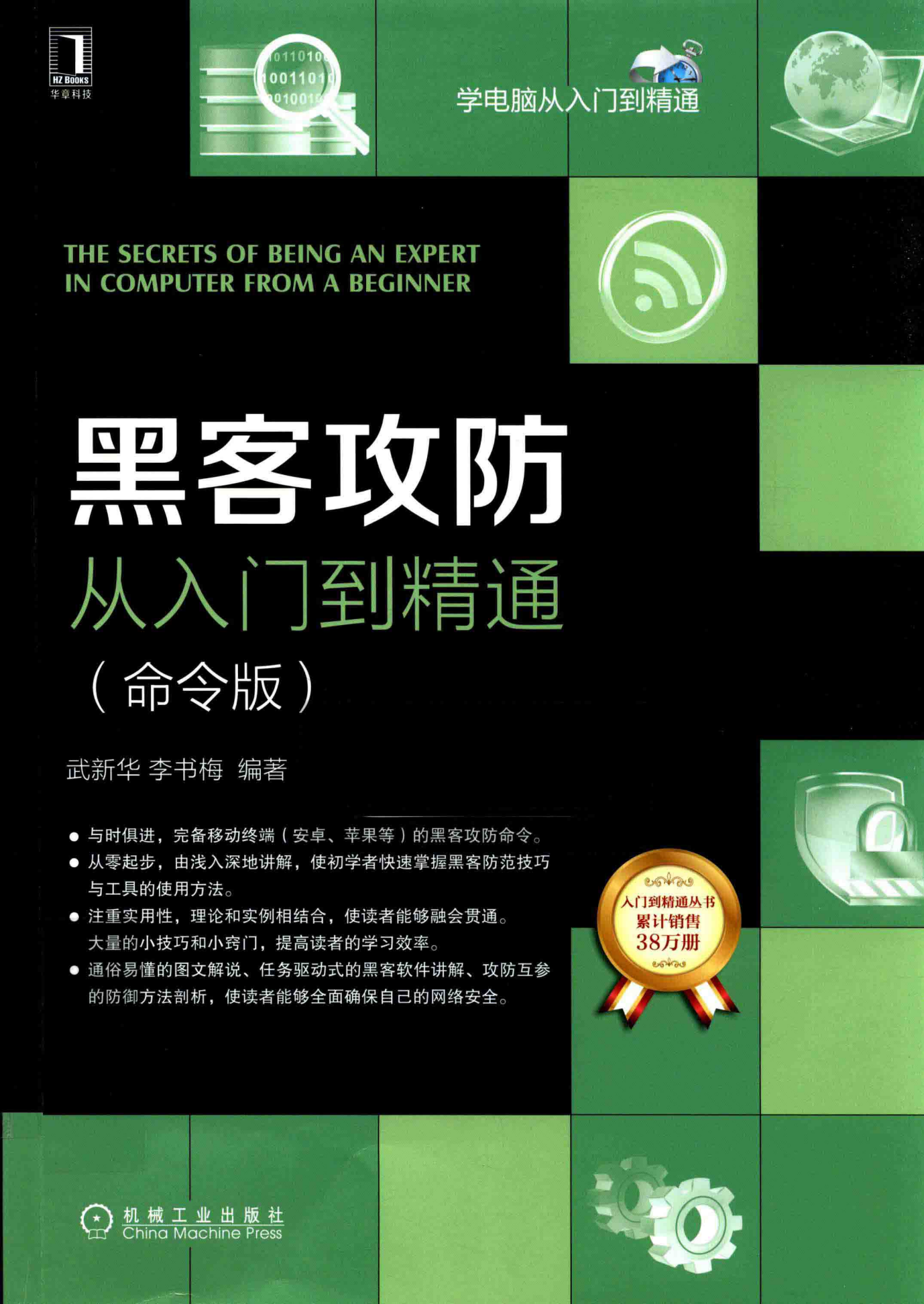
HZ BOOKS
华章科技
学电脑从入门到精通
THE SECRETS OF BEING AN EXPERT
IN COMPUTER FROM A BEGINNER
黑客攻防
从入门到精通
（命令版）
武新华 李书梅 编著
● 与时俱进，完备移动终端（安卓、苹果等）的黑客攻防命令。
● 从零起步，由浅入深地讲解，使初学者快速掌握黑客防范技巧与工具的使用方法。
● 注重实用性，理论和实例相结合，使读者能够融会贯通。大量的小技巧和小窍门，提高读者的学习效率。
● 通俗易懂的图文解说、任务驱动式的黑客软件讲解、攻防互参的防御方法剖析，使读者能够全面确保自己的网络安全。
入门到精通丛书
累计销售
38万册
机械工业出版社
China Machine Press

黑客攻防
从入门到精通
（命令版）

武新华 李书梅 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：命令版 / 武新华，李书梅编著 . —北京：机械工业出版社，2016.3
（学电脑从入门到精通）

ISBN 978-7-111-53279-8

I. 黑… II. ①武… ②李… 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（2016）第 053885 号

本书紧紧围绕黑客命令与实际应用展开，剖析在用户设备被黑客入侵时用户迫切需要用到或想要用到的命令，力求进行傻瓜式的讲解，使读者对网络入侵防御技术有系统了解，能够更好地防范黑客的攻击。全书共分为 15 章，包括：初识黑客、Windows 系统中的命令行、黑客常用的 Windows 网络命令行、Windows 系统命令行配置、基于 Windows 认证的入侵、远程管理 Windows 系统、局域网攻击与防范、DOS 命令的实际应用、制作启动盘、批处理 BAT 文件编程、病毒木马的主动防御和清除、流氓软件和间谍软件的清除、Android 操作系统的控制与安全、iOS 操作系统的常见应用及安全、移动 Wi-Fi 安全攻防等内容。

本书内容丰富、图文并茂、深入浅出，不仅适用于广大网络爱好者，而且适用于网络安全从业人员及网络管理员。

黑客攻防从入门到精通（命令版）

出版发行：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：张梦玲　　责任校对：董纪丽
印　　刷：北京瑞德印刷有限公司　　版　　次：2016 年 4 月第 1 版第 1 次印刷
开　　本：185mm×260mm　1/16　　印　　张：24.75
书　　号：ISBN 978-7-111-53279-8　　定　　价：69.00 元

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）88379426　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzit@hzbook.com

前言

黑客使用得最多、最频繁的工具不是那些 Windows 系统中的工具软件，而是那些被 Microsoft（微软）刻意摒弃的 DOS 命令，或者更具体地说，就是那些需要手工在命令行状态下输入的网络命令。因此，就有人不断发出“DOS 不是万能的，但没有 DOS 是万万不能的”感慨。

在计算机技术日新月异的今天，称霸天下的 Windows 系统仍有很多做不了和做不好的事，学习和掌握 DOS 命令行技术仍然是成为计算机高手的必修课程。

本书涵盖了 DOS 和 Windows 各版本操作系统下几乎所有的网络操作命令，详细地讲解了各种命令的功能和参数，并针对具体应用列举了大量经典示例，能使广大 Windows 用户知其然，更知其所以然，真正做到学以致用，技高一筹。

为了节省用户宝贵的时间，提高用户的使用水平，本书在创作过程中尽量具备如下特色：

- 与时俱进，加入移动终端（Android、iOS 等）安全方面内容的介绍。
- 从零起步，步步深入，由浅入深地讲解，使初学者和具有一定基础的用户都能逐步提高，快速掌握黑客防范技巧与工具的使用方法。
- 注重实用性，理论和实例相结合，并配以大量插图，生动易懂。
- 介绍大量小技巧和小窍门，提高读者的学习效率，节省他们的摸索时间。
- 重点突出、操作简单、内容丰富，同时附有大量的操作实例，读者可以一边学习，一边在计算机上操作，做到即学即用、即用即得。

本书内容全面、语言简练、深入浅出、通俗易懂，既可作为即查即用的工具手册，也可作为了解黑客的参考书目。本书不论在体例结构上，还是在技术实现及创作思想上，都做了精心的安排，力求将最新的技术、最好的学习方法奉献给读者。

作者采用通俗易懂的图文解说，即使你是计算机新手也能通读全书；用任务驱动式的黑客软件讲解，揭秘每一种黑客攻击的手法；新颖的黑客技术盘点，有助于你做好“先下手为强”的防护；攻防互参的防御方法，全面确保你的网络安全。

我们虽满腔热情，但限于自己的水平，书中的疏漏之处在所难免，欢迎广大读者批评指正。

编者

2016 年 1 月

目录

第4章 Windows系统命令行配置 / 72

第5章 基于Windows认证的入侵 / 96

第6章 远程管理Windows系统 / 146

第7章 局域网攻击与防范 / 165

第8章 DOS命令的实际应用 / 197

第9章 制作启动盘 / 219

第10章 批处理BAT文件编程 / 234

第11章 病毒木马的主动防御和清除 / 248

第12章 流氓软件和间谍软件的清除 / 277

第13章 Android操作系统的控制与安全 / 306

第1章 初识黑客

想要学习黑客知识，就得了解进程、端口、IP 地址以及黑客常见的术语和命令。本章正是针对初学者对这方面了解不多，专门做出讲解，从而帮助读者为后面的学习打好基础。

主要内容：

- 认识黑客
- 认识进程
- 在计算机中创建虚拟环境
- 认识 IP 地址
- 认识端口

1.1 认识黑客

1994 年以来，互联网在全球的迅猛发展为人们提供了方便、自由和无限的财富，政治、军事、经济、科技、教育、文化等各个方面都越来越网络化，并且上网逐渐成为人们生活、娱乐的一部分。可以说，信息时代已经到来，信息已成为物质和能量以外维持人类社会的第三资源，它是未来生活中的重要介质。随着计算机的普及和互联网技术的迅速发展，黑客也随之出现了。

1.1.1 什么是黑客

黑客的基本含义是一个拥有熟练计算机技术的人，但大部分媒体将计算机侵入者称为黑客，而实际上，黑客有如下几种：

白帽黑客是指有能力破坏计算机安全但不具恶意目的的黑客。白帽黑客一般遵守道德规范并常常试图同企业合作去改善所发现的计算机安全弱点。

灰帽黑客是指处于伦理和法律边缘的黑客。

黑帽黑客别称骇客，经常使用于区分黑帽黑客和一般（正面的）有理性的黑客。这个词流行于 1983 年，采用了“Safe Cracker”的相似发音，并且理论化为一个犯罪和黑客的混成语。

1.1.2 黑客的特点

黑客的一般特点是：有英文基础、知道常用的黑客术语和网络安全术语、能熟练使用常用的 DOS 命令和黑客工具，还会使用主流的编程语言及脚本。

在常见的黑客论坛中，经常会看到肉鸡、后门和免杀等词语，这些词语可以统称为黑客术语。除了掌握相关的黑客术语属于之外，黑客一般还掌握 TCP/IP 协议、ARP 协议等网络安全术语。

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不同的功能，利用 Ping 命令可以获取目标计算机的 IP 地址以及主机名。而黑客工具则是指黑客用来远程入侵或者查看目标计算机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。

主流的编程语言以及脚本语言主要有 5 类，如下：

（1）网页脚本语言（web page script language）

网页脚本语言就是网页代码，比如 HTML、Javascript、CSS、ASP、PHP、XML 等。

（2）解释型语言（Interpreted Language）

解释型语言包括 Perl、Python、REBOL、Ruby 等，也常被称为脚本语言，通常被用于和底层的操作系统沟通。这类语言的缺点是效率差、源代码外露，因此不适合用来开发软件产品，一般用于网页服务器中。

（3）混合型语言（Hybrid Language）

混合型语言的代表是 Java 和 C#，介于解释型和编译型之间。

（4）编译型语言（Compiling Language）

C/C++、Java 都是编译型语言。

（5）汇编语言（Assembly Language）

汇编语言是最接近于硬件的语言，不过现在用的人很少。

提示

程序语言的学习顺序建议如下。

如果完全没有程序经验，可照这个顺序学习：Javascript→解释型语言→混合型语言→编译型语言→汇编。

1.1.3 黑客常用术语

1. 肉鸡

肉鸡比喻那些可以随意被黑客控制的计算机，黑客可以像操作自己的计算机那样来操作它们，而不被对方所发觉。

2. 木马

本马指表面上伪装成正常的程序，但是当这些程序运行时，入侵者就会获取系统的整个控制权限。有很多黑客热衷于使用木马程序来控制别人的计算机，比如灰鸽子、黑洞、PcShare 等。

3. 网页木马

网页本马指表面上伪装成普通的网页文件或是将恶意的代码直接插入到正常的网页文件中，当有人访问时，网页木马就会利用对方系统或者浏览器的漏洞自动将配置好木马的服务端下载到访问者的计算机上来自动执行。

4. 挂马

挂马指在别人的网站文件里放入网页木马或者是将代码潜入到对方正常的网页文件里，以使浏览者中马。

5. 后门

后门是一种形象的比喻，黑客在利用某些方法成功地控制了目标主机后，可以在对方的系统中植入特定的程序，或者是修改某些设置。这些改动从表面上很难被察觉，但是黑客却可以使用相应的程序或者方法轻易地与这台计算机建立连接，重新控制这台计算机，这就好像黑客偷偷地配了一把主人房间的钥匙，可以随时进出房间而不被主人发现一样。通常，大多数的特洛伊木马程序都可以被入侵者用于制作后门。

6. IPC$

IPC$ 是共享“命名管道”的资源，它是为了让进程之间通信而开放的命名管道，可以通

过验证用户名和密码获得相应的权限，在远程管理计算机和查看计算机的共享资源时使用。

7. 弱口令

弱口令指那些强度不够，容易被猜解的口令，类似 123、abc 这样的口令（密码）。

8. Shell

Shell 指的是一种命令执行环境，比如，我们按下键盘上的“开始键 +R”组合键时会出现“运行”对话框，在里面输入“ cmd”会出现一个用于执行命令的黑窗口，这个就是 Windows 的 Shell 执行环境。

9. WebShell

WebShell 就是以 ASP、PHP、JSP 或者 CGI 等网页文件形式存在的一种命令执行环境，也可以将其称为一种网页后门。

10. 溢出

确切地讲，应该是“缓冲区溢出”。简单地解释就是程序对接收的输入数据没有执行有效的检测而导致错误，后果可能是程序崩溃或者是执行攻击者的命令。其大致可以分为两类：①堆溢出；②栈溢出。

11. 注入

由于程序员的水平参差不齐，相当大一部分应用程序存在安全隐患，用户可以提交一段数据库查询代码，根据程序返回的结果，获得某些想要的数据，这个就是 SQL 注入。

12. 注入点

注入点是可以实行注入的地方，通常是一个访问数据库的连接。根据注入点数据库运行账号的不同权限，你所得到的权限也不同。

13. 内网

内网通俗地讲就是局域网，比如网吧、校园网、公司内部网等。IP 地址如果是在以下三个范围之内，就说明我们是处于内网之中的：10.0.0.0 ～ 10.255.255.255、172.16.0.0 ～ 172.31.255.255、192.168.0.0 ～ 192.168.255.255。

14. 外网

外网直接连入互联网，可以与互联网上的任意一台计算机互相访问。

15. 免杀

免杀通过加壳、加密、修改特征码、加花指令等技术来修改程序，使其逃过杀毒软件的查杀。

16. 加壳

利用特殊的算法，改变 EXE 可执行程序或者 DLL 动态链接库文件的编码（比如实现压缩、加密），以达到缩小文件体积或者加密程序编码，甚至是躲过杀毒软件查杀的目的。目前较常用的壳有 UPX、ASPack、PePack、PECompact、UPack 等。

17. 花指令

花指令是几句汇编指令，可让汇编语句进行一些跳转，使得杀毒软件不能正常地判断病

毒文件的构造。通俗地讲，就是杀毒软件是从头到脚按顺序来查找病毒的，如果我们把病毒的头和脚颠倒位置，杀毒软件就找不到病毒了。

1.2 认识IP地址

在互联网中，只要利用IP地址，都可以找到目标主机，因此，如果想要攻击某个互联网主机，就要先确定该目标主机的域名或IP地址。

1.2.1 IP地址概述

所谓IP地址就是一种主机编址方式，给每个连接在互联网中的主机分配一个32 bit（比特）地址，也称为网际协议地址。

按照传输控制协议/Internet协议（Transport Control Protocol/Internet Protocol，TCP/IP）协议的规定，IP地址用二进制来表示，每个IP地址长32 bit，1 bit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“.”分为不同的字节，即用XXX.XXX.XXX.XXX的形式来表现，每组XXX代表小于等于255的10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（Dotted decimal notation）”，这显然比二进制的1或0容易记忆。

一个完整的IP地址信息通常应包括IP地址、子网掩码、默认网关和DNS等4部分内容。它们4个只有协同工作时，用户才可以访问互联网并被互联网中的计算机所访问（采用静态IP地址接入互联网时，ISP应当为用户提供全部的IP地址信息）。

1. IP地址

企业网络使用的合法IP地址，由提供互联网接入的服务商（ISP）分配，私有IP地址则可以由网络管理员自由分配。但网络内部所有计算机的IP地址都不能相同，否则，会发生IP地址冲突，导致网络连接失败。

2. 子网掩码

子网掩码是与IP地址结合使用的一种技术，其主要作用有两个，一是用于确定地址中的网络号和主机号，二是用于将一个大IP网络划分为若干个小子网络。

3. 默认网关

默认网关是指一台主机如果找不到可用的网关，就把数据包发送给默认指定的网关，由这个网关来处理数据包。从一个网络向另一个网络发送信息时，也必须经过一道“关口”，这道关口就是网关。

4. DNS

DNS服务用于将用户的域名请求转换为IP地址。如果企业网络没有提供DNS服务，则