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）

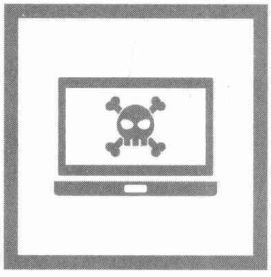
第2版

武新华 李书梅 孟繁华 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。

机械工业出版社
China Machine Press

学电脑从入门到精通

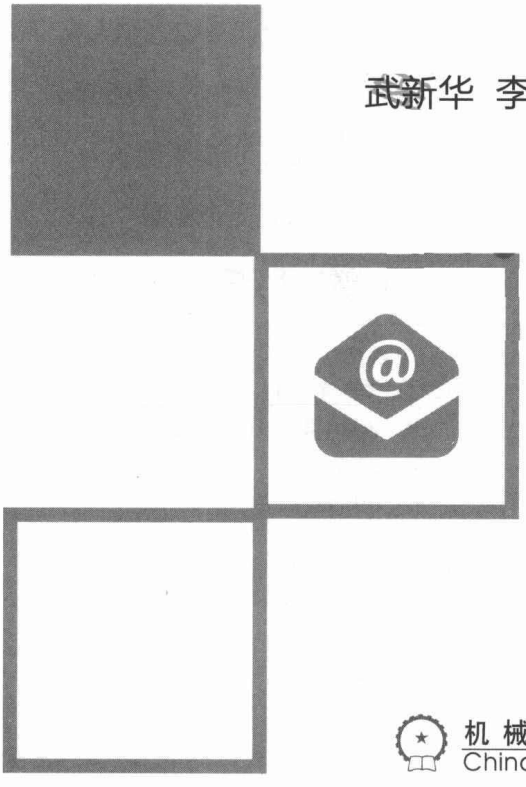


黑客攻防

从入门到精通

（命令版） 第2版

武新华 李书梅 孟繁华 编著



安徽理工大学 藏書 图書馆

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，孟繁华编著．—2 版．—北京：机械工业出版社，2020.5

ISBN 978-7-111-65492-6

I. 黑… II. ①武… ②李… ③孟… III. 黑客 - 网络防御 IV. TP393.081

中国版本图书馆 CIP 数据核字（2020）第 073703 号

黑客攻防从入门到精通（命令版）第 2 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：佘 洁
责任校对：李秋荣
印 刷：北京市荣盛彩色印刷有限公司
版 次：2020 年 6 月第 2 版第 1 次印刷
开 本：185mm × 260mm 1/16
印 张：20.75
书 号：ISBN 978-7-111-65492-6
定 价：69.00 元

客服电话：（010）88361066 88379833 68326294
投稿热线：（010）88379604
华章网站：www.hzbook.com
读者信箱：hzit@hzbook.com

版权所有 · 侵权必究
封底无防伪标均为盗版
本书法律顾问：北京大成律师事务所 韩光 / 邹晓东

此为试读，需要完整PDF请访问：www.ertongbook.com

前言

黑客最常用的工具不是 Windows 系统中的工具软件，而是那些被 Microsoft 刻意摒弃的 DOS 命令，或者更具体地说，是那些需要手工在命令行状态下输入的网络命令。因此，有人发出了“DOS 不是万能的，但没有 DOS 是万万不能的”这样的感慨。

在计算机技术日新月异的今天，Windows 系统仍有很多做不了和做不好的事情，学习和掌握 DOS 命令行技术仍然是进阶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实例，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。

为了节省读者宝贵的时间，提高读者的使用水平，本书在创作过程中尽量具备如下特色：

- 从零起步，通俗易懂，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，并配以大量插图和配套视频讲解，力图使读者融会贯通。
- 介绍了大量小技巧和小窍门，以提高读者的学习效率，节省读者宝贵的摸索时间。
- 重点突出、操作简练、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，让读者快速学会这些操作。

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，也可作为了解系统的参考书目。本书无论在体例结构上，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、最好的学习方法以最快的掌握速度奉献给读者。

笔者采用通俗易懂的图文解说，即使是计算机新手也能理解全书；通过任务驱动式的黑客软件讲解，揭秘每一种黑客攻击的手法；最新的黑客技术盘点，让你实现“先下手为强”；攻防互参的防御方法，全面确保你的网络安全。

笔者虽满腔热情，但限于自身水平，书中疏漏之处在所难免，欢迎广大读者批评指正。

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。本书的目的是希望读者了解黑客行为以更有效地保护自己，切记不要使用本书中介绍的黑客技术对别人的计算机进行攻击，否则后果自负！

目录

第5章 基于Windows认证的入侵 / 102

第8章 DOS命令的实际应用 / 196

第9章 操作系统的启动盘、安装、升级与修复 / 216

此为试读，需要完整PDF请访问：www.ertongbook.com

第10章 批处理文件编程 / 237

第11章 病毒和木马的主动防御和清除 / 251

第1章 初识黑客

想要学习黑客知识，就得了解进程、端口、IP 地址以及黑客常用的术语和命令。本章针对对这方面了解不多的初学者进行讲解，从而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测试环境
- 认识 IP 地址
- 认识端口

1.1 认识黑客

1994 年以来，因特网在全球的迅猛发展为人民提供了方便、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因特网技术的迅速发展，黑客也随之出现。

1.1.1 黑客的分类及防御黑客攻击应具备的知识

1. 黑客分类

黑客的基本含义是指一个拥有熟练计算机技术的人，但大部分的媒体认为“黑客”是指计算机侵入者。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。白帽子一般遵守道德规范并常常试图通过企业合作来改善被发现的安全弱点。

灰帽黑客是指使用计算机或某种产品系统中的安全漏洞，进而引起其拥有者对系统漏洞的注意。

黑帽黑客别称骇客，通常指系统或网络的非法入侵者。

2. 防御黑客攻击应具备的知识

知己知彼才能更好地做好防御，本节介绍防御黑客攻击应具备的知识。

（1）一定的英文水平

具备一定的英文水平对于防御黑客攻击来说非常重要，因为现在很多资料和教程都是英文版本，因此从一开始就要尽量阅读英文资料、使用英文软件，并且及时关注国外著名的网络安全网站。

（2）理解常用的黑客术语和网络安全术语

在常见的技术论坛中，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，如果不理解这些词语，则在与其他安全技术人员交流技术或经验时就会显得很吃力。除了掌握相关的黑客术语之外，还需要掌握 TCP/IP 协议、ARP 协议等网络安全术语。

（3）熟练使用常用的 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 等命令，利用这些命令可以实现对应的功能，如使用 ping 命令可以获取目标计算机的 IP 地址以及主机名。而黑客工具则是指黑客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

程序语言可分为以下 5 类。

- 网页脚本语言（Web Page Script Language）
  网页脚本语言包括 HTML、JavaScript、CSS、ASP、PHP、XML 等。
- 解释型语言（Interpreted Language）
  解释型语录包括 Perl、Python、REBOL、Ruby 等，也常称为脚本语言，通常用于与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。所以这类语言不适合用来开发软件产品，一般用于网页服务器。
- 混合型语言（Hybrid Language）
  混合型语言的代表是 Java 和 C#。介于解释型语言和编译型语言之间。
- 编译型语言（Compiling Language）
  C/C++、Java 都是编译型语言。
- 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

如果完全没有程序经验，可按照 JavaScript →解释型语言→混合型语言→编译型语言→汇编语言这个顺序学习。

1.1.2 黑客常用术语

1. 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操作它们，而不会被对方发觉。

2. 木马

木马是指表面上伪装成正常程序，但是当这些程序被运行时，就会获取系统的整个控制权限。有很多黑客就是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

网页木马是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的木马的服务端下载到访问者的计算机上并自动执行。

4. 挂马

挂马是指在别人的网站文件里放入网页木马或者将代码潜入对方正常的网页文件里，以使浏览者中马。

5. 后门

这是一种形象的比喻，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，或者修改某些设置。这些改动表面上是很难被察觉的，但是黑客却可

以使用相应的程序或者方法来轻易地与这台计算机建立连接，重新控制这台计算机，就好像是黑客偷偷地配了一把主人房间的钥匙，可以随时进出而不被主人发现一样。通常大多数特洛伊木马程序都可以被入侵者用于语制作后门。

6. IPC$

IPC$ 是共享“命名管道”的资源，它是为进程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

弱口令是指那些强度不够，容易被猜解的，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”时出现“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，这个黑窗口就是 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，也可以将其称为是一种网页后门。

10. 溢出

确切来讲，溢出指“缓冲区溢出”。简单的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的错误，后果可能是造成程序崩溃或者执行攻击者的命令。溢出大致可以分为两类：①堆溢出；②栈溢出。

11. SQL 注入

由于程序员的水平参差不齐，相当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，并根据程序返回的结果获得某些他想要的数据，这就是 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权限的不同，你所得到的权限也不同。

13. 内网

通俗来讲，内网就是局域网，比如网吧、校园网、公司内部网等都属于内网。查看 IP 地址时如果在以下三个范围之内，就说明我们是处于内网之中：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

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，将 EXE 可执行程序或者 DLL 动态链接库文件的编码进行改变（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，可以让汇编语句进行一些跳转，使得杀毒软件不能正常判断病毒文件的构造。通俗点就是，杀毒软件是从头到脚按顺序来查找病毒，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，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

IP 地址就是一种主机编址方式，每个连接在 Internet 上的主机可分配一个 32 位（比特）地址，也称网际协议地址。

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 32 位，即 4 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形式，中间使用符号“.”以分为不同的字节，即用 XXX.XXX.XXX.XXX 的形式来表现，每组 XXX 代表小于或等于 255 的十进制数，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。

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 四部分内容。这四部分内容只有协同工作时，用户才可以访问 Internet 并被 Internet 中的计算机访问（采用静态 IP 地址接入 Internet 时，ISP 应当为用户提供全部 IP 地址信息）。

1. IP 地址

企业网络使用的合法 IP 地址由提供 Internet 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 网络划分为若干个子网络。

此为试读，需要完整PDF请访问：www.ertongbook.com