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

实战篇

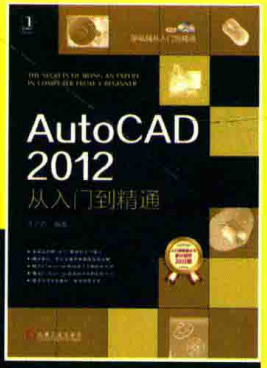
第2版

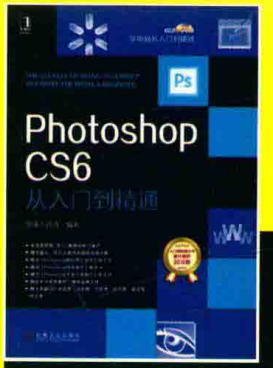
王叶 李瑞华 孟繁华 编著

- 简单易学：从易到难、循序渐进，图文并茂、通俗易懂
- 实用性强：网络真实攻防技术、案例+技术的讲解模式
- 技巧与窍门：丰富的攻防技巧与窍门、帮读者答疑解惑，掌握攻防技术

机械工业出版社
China Machine Press

学电脑从入门到精通





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

华章网站：www.hzbook.com
网上购书：www.china-pub.com
数字阅读：www.hzmedia.com.cn

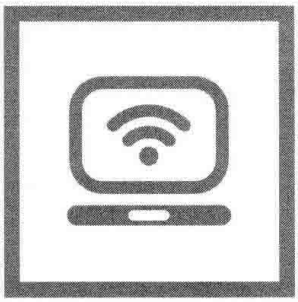
上架指导：计算机/安全

ISBN 978-7-111-65538-1

9 787111 655381 >

定价：69.00元

学电脑从入门到精通

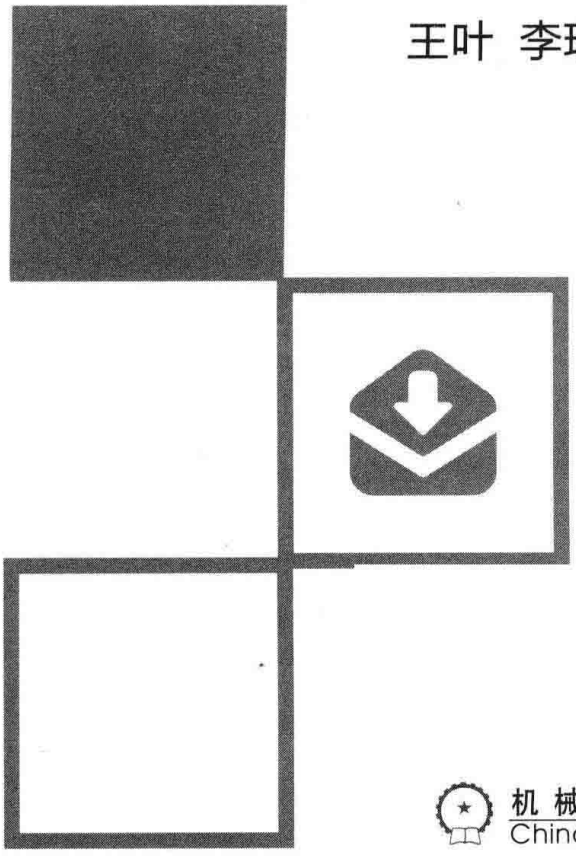


黑客攻防

从入门到精通

实战篇 第2版

王叶 李瑞华 孟繁华 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：实战篇 / 王叶，李瑞华，孟繁华编著 .—2 版 . —北京：机械工业出版社，2020.5

ISBN 978-7-111-65538-1

I. 黑… II. ①王… 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 081239 号

黑客攻防从入门到精通　实战篇　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：余　洁　　责任校对：李秋荣

印　　刷：三河市宏图印务有限公司　　版　　次：2020 年 6 月第 2 版第 1 次印刷

开　　本：185mm × 260mm　1/16　　印　　张：21.75

书　　号：ISBN 978-7-111-65538-1　　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

华章图书

一本打开的书，
一扇开启的门，
通向科学殿堂的阶梯，
托起一流人才的基石。

前言

如今，网上消费、投资、娱乐等已占据了我们生活的一大部分，如何保证网络账户、密码安全已成为广大用户非常关注的问题，尤其是经常听闻身边好友 QQ 被盗、账号丢失等，防御黑客入侵已经成为一个不得不重视的问题，因而作者编写了此书。

本书主要内容

本书共分为 14 章，主要内容如下：

第 1 章：认识黑客并介绍学习黑客攻防前首先要了解的基础知识，包括 IP 地址、端口、黑客常见术语及命令，以及曝光黑客在攻击前做的准备工作——创建虚拟测试环境。

第 2 章：介绍黑客攻击前对信息的扫描与嗅探以及网络监控技巧。

第 3 章：介绍系统常见漏洞攻击与防御技巧。

第 4 章：认识病毒并介绍病毒入侵与防御技巧，同时曝光简单病毒的制作过程。

第 5 章：认识木马并介绍木马的伪装与生成、加壳与脱壳以及木马的清除。

第 6 章：介绍通过入侵检测技术自动检测可疑行为，在系统受到危害前发出警告，防患于未然。

第 7 章：介绍代理和日志清除技术，此为黑客入侵常用的隐藏和清除入侵痕迹的手段。

第 8 章：介绍几种常见的远程控制技术，如今该技术在远程教育、远程协助、远程维护等方向应用较多。

第 9 章：介绍 NTFS 文件、多媒体、Word 文件、光盘等的常见加密 / 解密技术，

以及几种常用的加密 / 解密工具。

第 10 章：介绍常见的网络欺骗方式以及防范方法。

第 11 章：介绍 SQL 注入、网络钓鱼等常见网站攻击手法，并给出了预防措施。

第 12 章 ：介绍系统和数据的备份与恢复，在系统遭受木马病毒攻击而无法使用时，备份与恢复就能够发挥其作用。

第 13 章：介绍间谍软件的清除和系统清理，以保证系统环境更加安全。

第 14 章 ：介绍常用购物软件、银行 APP 软件的安全防护措施，以及常用手机安全软件的设置。

本书特色

- 简单易懂。本书内容从零起步，由浅入深，适用于初次接触黑客攻防技术的读者。
- 实用性强。本书理论和实例相结合，并配以大量插图，步骤解释明晰，让读者能够一目了然，轻松学习。
- 小技巧和小窍门。帮助读者答疑解惑，提高学习效率。

本书语言简练，内容丰富，并配有大量操作实例，综合作者使用经验和操作心得，可以作为个人学习和了解黑客攻防知识的参考书籍。

最后，感谢广大读者的阅读与支持，鉴于水平有限，书中难免存在疏漏之处，欢迎批评指正。

目录

第11章 网站攻击与防范 / 228

第12章 系统和数据的备份与恢复 / 251

第13章 间谍软件的清除和系统清理 / 290

第14章 如何保护手机财产安全 / 326

第1章 从零开始认识黑客

主要内容：

- 认识黑客
- 认识端口
- 在计算机中创建虚拟测试环境
- 认识 IP 地址
- 黑客常见术语与命令

1.1 认识黑客

1.1.1 白帽、灰帽和黑帽黑客

自 1994 年以来，因特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、文化等各个方面与网络的结合也越来越紧密，网络也由此逐渐成为人们生活的一部分。可以说，信息时代已经到来，信息作为物质和能量以外维持人类社会运转的第三资源，正体现出越来越重要的作用，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。

黑客的原本含义是指拥有熟练计算机技术的人，但现今大部分的媒体提到的“黑客”指计算机侵入者。其中黑客又可分为白帽黑客、灰帽黑客和黑帽黑客。

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。白帽子一般有清楚定义的道德规范，并常常试图同企业合作来改善被发现的安全弱点。

灰帽黑客是指对于伦理和法律暧昧不清的黑客。

黑帽黑客这个词自 1983 年开始流行，采用了 safe cracker 的解释，并且理论化为一个犯罪和黑客的混合语。

1.1.2 黑客、红客、蓝客和骇客

黑客：最早源自英文 hacker，他们都是水平高超的计算机专家，尤其指程序设计人员，是一个统称。

红客：维护国家利益的黑客，他们热爱自己的祖国、民族、和平，极力维护国家安全与尊严。

蓝客：信仰自由、提倡爱国主义的黑客，用自己的力量来维护网络的和平。

骇客：是“ Cracker”的音译，就是“破解者”的意思，从事恶意破解商业软件、恶意入侵别人的网站等活动。

1.2 认识 IP 地址

在网络中，每一台主机也有一个“地址”，这就是 IP 地址。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

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 32bit(位)

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 / 网际协议）的规定，IP 地址用二进制来表示，每个 IP 地址长 32bit，换算成字节就是 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“.”来分为不同的字节，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，例如 192.168.38. 6，这显然比二进制的 1 或 0 容易记忆多了。

一条完整的 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。只有四者协同工作时，用户才可以访问 Internet 并被 Internet 中的计算机所访问（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

子网掩码要与 IP 地址结合使用，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的子网络。

3. 默认网关

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，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 DNS 服务器的 IP 地址应当指向 ISP 的 DNS 服务器。如果企业网络自己提供了 DNS 服务，则 DNS 服务器的 IP 地址就是内部 DNS 服务器的 IP 地址。

1.2.2 IP 地址的分类

互联网中的每个接口有一个唯一的 IP 地址与其对应，该地址具有一定的结构，一般情况下，IP 地址可以分为 5 大类，即 A 类、B 类、C 类、D 类以及 E 类。

这些 32 位的地址通常写成 4 个十进制的数，其中每个整数对应一字节。这种表示方法称为“点分十进制表示法”(dotted decimal notation)。

1. A 类 IP 地址

A 类 IP 地址由 1 字节的网络地址和 3 字节的主机地址组成，网络地址的最高位必须是“0”。可用的 A 类网络有 126 个，每个网络能容纳 1 亿多个主机（网络号不能为 127，因为该网络号被保留用作回路及诊断功能），地址范围为 1.0.0.1 ～ 126.155.255.254。