基础入门 工具使用 攻防技巧 实战演练

黑客技术新手、爱好者一定要看的*最佳工具书*

最新案例实战版

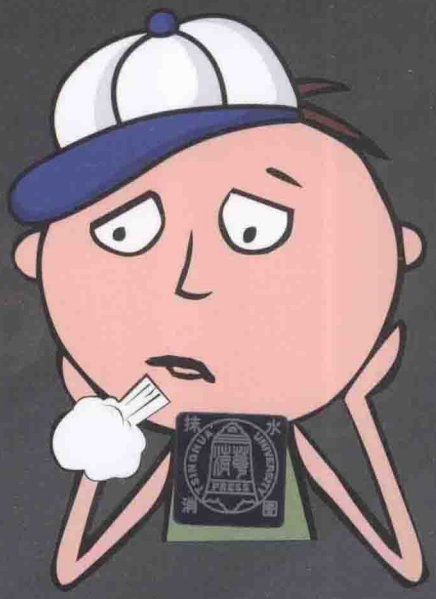
玩转黑客攻防

从入门到精通

少 侠 编著

PC、手机、Wi-Fi……

经典热门黑客攻防技术 全搞定



超值视频课程免费下载

清华大学出版社

玩转

黑客攻防

从入门到精通

少 侠 编著

清华大学出版社
北 京

内 容 简 介

本书由易到难、循序渐进地介绍了黑客入侵攻击及防御黑客入侵攻击的基础知识及应用技巧，主要包括黑客入门基础知识、扫描和嗅探的实施与防范、防范与清除电脑病毒、防范与清除电脑木马、移动设备黑客攻击与防范、Wi-Fi 攻击与防范、文件加密与解密、Windows 系统漏洞入侵防范、局域网攻击与防范、账号盗取与安全防范、网站常见攻击方式、系统远程控制与反控制、网络代理与追踪、后门的创建与检测、黑客入侵检测、清理入侵痕迹、系统清理与间谍软件的清除、网络支付工具安全防范、系统和数据的备份与恢复共 19 章内容。本书重点在学习黑客入侵的基础上，掌握如何采取有效的防范措施，还介绍了移动设备与 Wi-Fi 等热点技术与应用。

本书适用于黑客技术初学者和爱好者，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和培训机构。

图书在版编目（CIP）数据

玩转黑客攻防从入门到精通 / 少侠编著. —北京：清华大学出版社，2015

ISBN 978-7-302-39867-7

Ⅰ. ①玩… Ⅱ. ①少… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2015）第 080716 号

责任编辑：王金柱
封面设计：王　翔
责任校对：闫秀华
责任印制：何　芊

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：190mm×260mm　　**印　　张**：27.5　　**字　　数**：704 千字
版　　次：2015 年 6 月第 1 版　　**印　　次**：2015 年 6 月第1次印刷
印　　数：1～3500
定　　价：69.00 元

产品编号：064011-01

前　言

如今网上购物、投资、理财等已经占据了很大的消费市场，财产的安全性也越来越重要，如果账户、密码被黑客截取，将会带来很大的损失。而计算机网络的普及、黑客工具的传播，使得只需简单的工具，就能够对一些疏于防范的电脑或终端进行攻击，并在受侵入的电脑或终端里为所欲为。当发现自己的密码被盗、资料被修改删除、硬盘变作一片空白之时，再想亡羊补牢，为时已晚。

本书内容

本书从“攻”、“防”两个不同的角度讲解黑客攻击手段的同时，介绍了相应的防范方法，图文并茂地再现了网络入侵与防御的全过程。本书内容涵盖了黑客入门基础知识、扫描和嗅探的实施与防范、电脑安全防范、移动设备黑客攻击与防范、Wi-Fi 攻击与防范、文件加密与解密、Windows 系统漏洞入侵防范、局域网攻击与防范、账号盗取与安全防范、网站常见攻击方式、系统远程控制与反控制、网络代理与追踪、后门的创建与检测、黑客入侵检测、清理入侵痕迹、系统清理与间谍软件的清除、网络支付工具安全防范、系统和数据的备份与恢复等，让读者在了解黑客如何攻击的同时学习到如何拒敌于千里的方法。

本书还在各章安排了实战演练案例，读者可以边学边练，提高实战技能。

本书特色

本书由浅入深地讲解了黑客攻击和防范的具体方法和技巧，通过具体形象的案例向读者展示了多种攻击方法和攻击工具的使用。通过完成实践任务，读者可以轻松掌握各种知识点，在不知不觉中快速提升防范黑客的实战技能。

- 任务驱动，自主学习，理论+实战+图文=让读者快速精通。
- 讲解全面，轻松入门，快速打通初学者学习的重要关卡。
- 实例为主，易于上手，模拟真实工作环境，解决各种疑难问题。

本书以实例分析加案例剖解为主要脉络，以图文并茂、按图索骥方式详细讲解黑客的攻击手法和相应的网络安全管理防御技术，并采用案例驱动的写作方法，照顾初级读者，详细分析每一个操作案例，力求通过一个知识点的讲解，实现读者用更少的时间快速掌握黑客技术，理解和掌握类似场合的应对思路。

提供教学视频下载

为方便初学者尽快上手，节省学习时间，本书还录制了部分章节的教学视频，提供共 64 段教学视频操作录像，读者可在电脑上直接播放观看。视频下载地址：http://pan.baidu.com/s/1c0gy51Y。

本书适合人群

本书适合如下读者学习使用：

- 使用电脑的广大读者；
- 需要获得数据保护的日常办公人员；
- 热衷黑客技术的初学者及安全技术的爱好者；
- 网络管理人员、网吧工作人员。

由于时间紧迫，水平有限，书中难免存在疏漏和不当之处，敬请读者批评指正，在您使用本书的过程中如遇到问题，请联系 QQ：3113088。

编　者

2015 年 3 月

目 录

第 1 章
黑客入门基础知识

小呆：我的电脑最近老出问题，专家说中病毒了，所以想要学习一些黑客知识做预防，可是找了一些书籍，都不怎么能看懂，怎么办？

少侠：别担心，你了解过黑客常见的一些术语与命令吗？比如术语有肉鸡、木马，还有后门等等；命令有 ping 命令、netstat 命令、Net 命令等。

小呆：木马我知道，但是肉鸡和后门就不知道了。至于命令，我都不太了解。难道我要先了解这些吗？

少侠：是这样。学习黑客知识前，首先要了解黑客常见的术语与命令，不止这些，进程、端口、IP 地址等基础知识也是很必要的。

小呆：多谢少侠，那么我就先从这些基础知识开始学起吧。

1.1 认识黑客

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。随着电脑的普及和因特网技术的迅速发展，黑客也随之出现了。

1.1.1 白帽、灰帽及黑帽黑客

黑客的基本涵义是指拥有熟练电脑技术的人，但大部分人将“黑客”用于电脑侵入者。

白帽黑客是指有能力破坏电脑安全但不具恶意目的的黑客。白帽黑客一般有清楚的道德规范，并常常试图同企业合作去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。

黑帽黑客和黑帽怪客经常用来区分黑帽黑客和一般（正面的）有理性的黑客。这个词自 1983 年开始流行，大概是由于采用了相似发音和对 safe cracker 的解释，并且理论化为一个犯罪和黑客的混成语。

1.1.2 黑客、红客、蓝客及骇客

黑客，最早源自英文 hacker，是指水平高超的电脑专家，尤其是程序设计人员，算是一个统称。

红客，是维护国家利益，不去利用网络技术入侵自己国家电脑，而是维护正义，为自己国家争光的黑客。

蓝客，是提倡爱国主义的黑客们，经常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。经常从事恶意破解商业软件、恶意入侵别人的网站等事务。

1.1.3 成为黑客必须掌握的知识

成为黑客，并不是一件简单的事情，不仅要熟练掌握一定的英文、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，而且要掌握主流的编程语言以及脚本。

1. 熟练掌握一定的英文

学习英文对于黑客来说非常重要，因为现在很多资料和教程都是英文版本，一个漏洞从发现到出现中文介绍，需要大约一个星期的时间，在这段时间内网络管理员就已经有足够的时间修补漏洞了，所以当看到中文介绍时，这个漏洞可能早就已经不存在了。因此学习黑客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，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显得很吃力。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不同的功能，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 5 类。

（1）Web Page Script Languages

就是网页代码，比如 HTML、JavaScript、CSS、ASP、PHP、XML 等。

（2）Interpreted Languages（解释型语言）

包括 Perl、Python、REBOL、Ruby 等，也常被称作 Script 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，所以不适合用来开发软件产品，一般用于网页服