网络安全技术丛

天河文化 编著

# 最新黑客攻防从入门到精通

## The Newest Hacker Attack and Defense: from Novice to Master


**内容全面，与时俱进：**
介绍手机黑客攻防、木马攻防等内容，帮助读者快速打通学习的重要关卡，轻松入门。

**任务驱动，自主学习：**
“理论 + 实战 + 图文 + 视频”的学习模式，让读者快速精通黑客攻防技术。

**实例为主，易于上手：**
模拟真实的工作环境，解决各种疑难问题。

机械工业出版社
CHINA MACHINE PRESS

网络安全技术丛书

# 最新黑客攻防从入门到精通

天河文化　编著

机械工业出版社

本书共 19 章，结合案例，由浅入深、系统全面地介绍了黑客攻防技术，内容涵盖：从零开始认识黑客、信息的扫描与嗅探、系统漏洞攻防、病毒攻防、木马攻防、手机黑客攻防、网游与网吧攻防、密码攻防、黑客入侵检测技术、网络代理与追踪技术、后门技术、入侵痕迹清除技术、远程控制技术、局域网攻防、QQ 账号攻防、网站攻防、系统和数据的备份与恢复、保障网络支付工具的安全、间谍软件的清除和系统清理。

本书内容丰富全面、图文并茂、从易到难，面向广大计算机初学者和黑客攻防技术爱好者，也适用于需要保障数据安全的日常办公人员、网络安全从业人员及网络管理人员参考阅读。

**图书在版编目（CIP）数据**

最新黑客攻防从入门到精通 / 天河文化编著. —北京：机械工业出版社，2015.3

（网络安全技术丛书）

ISBN 978-7-111-49787-5

Ⅰ. ①最… Ⅱ. ①天… 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 061306 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）

策划编辑：王海霞

责任编辑：王海霞 责任校对：张艳霞

责任印制：乔 宇

保定市中画美凯印刷有限公司印刷

2015 年 5 月第 1 版 • 第 1 次印刷

184mm×260mm • 26 印张 • 643 千字

0001－4000 册

标准书号：ISBN 978-7-111-49787-5

ISBN 978-7-89405-745-7（光盘）

定价：69.80 元（含 1CD）

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务

服务咨询热线：（010）88361066

读者购书热线：（010）68326294

（010）88379203

网络服务

机 工 官 网：www.cmpbook.com

机 工 官 博：weibo.com/cmp1952

教育服务网：www.cmpedu.com

金 书 网：www.golden-book.com

# 前言

随着互联网的普及，人们越发地依赖利用互联网进行购物和投资等，互联网的发展同时方便了黑客工具的传播，有的黑客会对一些疏于防范的计算机做出攻击，进行识别偷窃、窃取信用卡账号、勒索银行等行为。因此，提高防范意识，学习黑客的入侵手段以及防御黑客的技术和方法极为重要。

## 本书内容

本书紧紧围绕“攻”和“防”两个不同的角度，先揭露黑客攻击手段，再介绍相应的防范方法。知己知彼，方能更好地防御黑客攻击。

本书内容共 19 章。

第 1 章：从零开始认识黑客。主要介绍黑客基础知识，包括黑客常用术语、进程、端口、常见的网络协议、黑客常用命令以及在计算机中创建虚拟测试环境等内容。

第 2 章：信息的扫描与嗅探。主要介绍扫描、嗅探的实施与防范以及网络监控等内容。

第 3 章：系统漏洞攻防。主要介绍系统漏洞基础知识、Windows 服务器系统入侵曝光、DcomRpc 漏洞入侵曝光以及用 MBSA 检测系统漏洞等内容。

第 4 章：病毒攻防。主要介绍病毒基础知识、两种简单病毒的生成与防范、脚本病毒的生成与防范、宏病毒与邮件病毒的防范、网络蠕虫的防范以及杀毒软件的使用等内容。

第 5 章：木马攻防。主要介绍木马基础知识、木马的伪装与生成、木马的加壳与脱壳以及木马清除软件的使用等内容。

第 6 章：手机黑客攻防。主要介绍智能手机操作系统、获取 Android Root 权限、Android 手机备份功能、安卓系统刷机、苹果手机越狱、手机蓝牙攻击曝光、手机拒绝服务攻击曝光、手机电子邮件攻击曝光、手机病毒与木马攻防、手机加密技术、手机支付安全防范、手机优化及安全性能的提升等内容。

第 7 章：网游与网吧攻防。主要介绍网游盗号木马、网站充值欺骗术、防范游戏账号破解、警惕局域网监听及美萍网管大师等内容。

第 8 章：密码攻防。主要介绍加密与解密基础知识、七种常见的加密解密类型、文件和文件夹密码攻防、系统密码攻防及其他加密解密工具等内容。

第 9 章：黑客入侵检测技术。主要介绍基于网络的入侵检测系统、基于主机的入侵检测系统、基于漏洞的入侵检测系统、萨客嘶入侵检测系统、Snort 入侵检测系统等内容。

第 10 章：网络代理与追踪技术。主要介绍网络代理工具“代理猎手”和 SocksCap32、常见的黑客追踪工具 NeroTrace Pro 等内容。

第 11 章：后门技术。主要介绍后门的分类、账号后门技术曝光、系统服务后门技术曝光、检测系统中的后门程序等内容。

第 12 章：入侵痕迹清除技术。主要介绍黑客留下的脚印、清除服务器日志、Windows 日志清理工具、清除历史痕迹等内容。

第 13 章：远程控制技术。主要介绍认识远程控制、远程桌面连接与协助、用 WinShell 实现远程控制、用 QuickIP 进行多点控制等内容。

第 14 章：局域网攻防。主要介绍局域网安全、局域网攻击曝光、局域网监控工具等内容。

第 15 章：QQ 账号攻防。主要介绍三种盗取 QQ 号码软件防范、用密码监听器揪出“内鬼”、保护 QQ 密码和聊天记录等内容。

第 16 章：网站攻防。主要介绍 SQL 注入攻击曝光、ZBSI 检测注入点曝光、Cookie 注入攻击曝光、跨站脚本攻击曝光等内容。

第 17 章：系统和数据的备份与恢复。主要介绍备份与还原操作系统、备份与还原用户数据、使用恢复工具来恢复误删除的数据等内容。

第 18 章：保障网络支付工具的安全。主要介绍加强支付宝的安全防护和加强财付通的安全防护等内容。

第 19 章：间谍软件的清除和系统清理。主要介绍流氓软件的清除、间谍软件防护实战和常见的网络安全防护工具等内容。

## 本书特色

本书循序渐进地讲解了黑客攻防的具体方法和技巧，通过完成一个个实践任务，读者可以轻松掌握各种知识点，在不知不觉中快速提升实战技能。

- 任务驱动，自主学习，“理论+实战+图文”学习模式让读者快速入门。
- 内容全面，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。

本书以图文并茂、按图索骥的方式揭露黑客的攻击手法，并详细讲解相应的网络安全管理防御技术，详细分析每一个操作案例，力求让读者尽快掌握黑客编程技术，理解和掌握类似场合的应对思路。

## 本书适合人群

本书适合以下读者学习使用：

- 计算机初学者；
- 需要保障数据安全的日常办公人员；
- 网络管理人员、网吧工作人员；
- 喜欢钻研黑客攻防技术但编程基础薄弱的读者；
- 相关计算机培训机构的师生。

## 本书作者

本书由天河文化编著，参与本书编写的人员有郑奎国、王叶、候琴琴、邵朝怡、施亚、宫晨伟、朱伟伟、李季、郑林、张阮阮、丁建飞、方开庆、陈红、陈伟、赵雨、王越、赵根昌、竹简、苗玉珍和余东航。

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计算机及相关设备的行为都属于违法行为，希望读者在阅读本书后不要使用本书中介绍的黑客技术侵害别人权益，否则后果自负。

编　者

# 目 录

## 第19章 间谍软件的清除和系统清理 / 379

# 第1章 从零开始认识黑客

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。由于初学者对这方面知识了解不多，本章专门针对上述内容进行讲解，从而帮助读者为后面的学习打好基础。

**要点提示**

- 黑客常用术语
- 进程和端口
- 常见的网络协议
- 黑客常用命令
- 创建虚拟测试环境