HZ BOOKS
华章科技

图文详解，轻松掌握
电脑\智能手机全适用

黑客攻防极速入门

黑客知识、常用命令与工具实战
电脑与手机黑客攻防秘技全曝光

张阮阮 等编著

知彼知己，百战不殆。

——《孙子兵法·谋攻篇》

机械工业出版社
China Machine Press

黑客攻防极速入门

张阮阮 等编著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

黑客攻防极速入门/张阮阮等编著. —北京：机械工业出版社，2016.5

ISBN 978-7-111-53812-7

Ⅰ. ①黑… Ⅱ. ①张… 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（2016）第110265号

本书全面详细地介绍了计算机及智能移动设备的黑客攻防常用技术，并提供了大量实用工具和操作案例。本书分为四篇：第一篇介绍黑客攻防基础，包括黑客攻防入门、黑客攻击手段揭秘、黑客攻防命令揭秘、黑客攻防学习环境搭建等知识；第二篇介绍计算机黑客攻防实战，包括扫描与嗅探、病毒攻防、木马攻防、Windows 系统漏洞攻防、后门攻防、局域网攻防、流氓软件与间谍软件攻防、远程控制攻防、加密与解密、数据备份与还原等知识；第三篇介绍无线与移动设备安全，包括无线网络 WiFi 攻防、手机黑客攻防等知识；第四篇介绍网游账号攻防、QQ 与 E-mail 账号攻防、网络支付工具安全等知识。

本书通俗易懂，图文并茂，适用于黑客及安全技术初学者、爱好者，也适用于企事业单位从事网络安全与维护的各类读者。

黑客攻防极速入门

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：夏非彼　迟振春

印　　刷：中国电影出版社印刷厂　　版　　次：2016 年 7 月第 1 版第 1 次印刷

开　　本：188mm × 260mm　1/16　　印　　张：24.5

书　　号：ISBN 978-7-111-53812-7　　定　　价：59.00 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

本书紧紧围绕“攻”与“防”两个不同的角度，图文并茂地介绍了网络入侵与防御的全过程，以帮助网络和计算机安全人员及爱好者了解黑客入侵的各种手段，找到防范方法，确保计算机与网络的安全。

本书内容

本书分为 4 篇：第一篇介绍黑客攻防基础，包括黑客攻防入门、黑客攻击手段揭秘、黑客攻防命令揭秘、黑客攻防学习环境搭建等知识；第二篇介绍计算机黑客攻防实战，包括扫描与嗅探、病毒攻防、木马攻防、Windows 系统漏洞攻防、后门攻防、局域网攻防、流氓软件与间谍软件攻防、远程控制攻防、加密与解密、数据备份与还原等知识；第三篇介绍无线与移动设备安全，包括无线网络 WiFi 攻防、手机黑客攻防等知识；第四篇介绍网游账号攻防、QQ 与 E-Mail 账号攻防、网络支付工具安全等知识。

本书特色

本书由浅入深地讲解了黑客入侵和防范的具体方法和技巧，通过具体形象的案例介绍向读者展示了入侵及防御方法和各种工具的使用。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=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。

本书适合人群

- 黑客及安全技术初学者、爱好者；
- 需要获得数据保护的日常办公人员；
- 企业网络管理人员、网吧工作人员；
- 家庭计算机用户及智能手机用户；
- 培训班。

本书主要由张阮阮编著，王鲁德、郑志华、王栋、宗立波、张辰、胡华、信传奇、李阳、王星凯等也参加了部分章节的编写。

由于编者水平所限，书中难免存在不足之处，敬请广大读者批评指正。

编者

2016 年 5 月

目 录

第二篇 计算机系统黑客攻防

第三篇　无线网络及智能手机黑客攻防

第四篇 网游、QQ、E-mail 及理财安全防范

第一篇　黑客攻防基础

第1章　从零开始认识黑客

黑客一词，源于英文 Hacker，原指热心于计算机技术，水平高超的电脑专家，尤其是程序设计人员。但到了今天，黑客一词已被用于泛指那些专门利用电脑搞破坏或恶作剧的家伙。想要打败黑客维护我们的信息安全，我们就要知己知彼，从真正意义上了解黑客，本章将会带你走进黑客的世界，带领你了解进程、端口、IP 地址以及黑客常见的术语和命令，从而帮助读者为后面的学习打好基础。

1.1　认识黑客

1.1.1　区别黑客、红客、蓝客、骇客及飞客

黑客，最早源自英文 hacker，原指热心于计算机技术、水平高超的电脑专家，尤其是程序设计人员，但到了今天，黑客一词已被用于泛指那些专门利用电脑搞破坏或恶作剧的家伙。

红客可以说是中国黑客起的名字，英文“honker”是红客的译音。通常红客是一群为捍卫中国主权而战的黑客们。他们热爱自己的祖国，热爱民族，热爱和平，极力的维护国家安全与尊严。

“蓝客”一词由中国蓝客联盟在 2001 年 9 月提出，他们信仰自由，提倡爱国主义，用自己的力量来维护网络和平。

骇客，是“Cracker”的音译，就是“破解者”的意思。他们主要从事恶意破解商业软件、恶意入侵别人的网站等事务。

黑客和骇客根本的区别是：黑客们建设，而骇客们破坏。

飞客是电信网络的先行者，他们经常利用程控交换机的漏洞进入并研究电信网络。

1.1.2 认识白帽、灰帽及黑帽黑客

白帽黑客，是指那些专门研究或者从事网络、计算机技术防御的人，他们通常受雇于各大公司，是维护网络、计算机安全的主要力量。很多白帽还受雇于公司，对产品进行模拟黑客攻击，以检测产品的可靠性。

灰帽黑客是指那些懂得技术防御原理，并且有实力突破这些防御的黑客。尽管他们的技术实力往往要超过绝大部分白帽和黑帽，但灰帽通常并不受雇于大型企业，他们往往将黑客行为作为一种业余爱好或者是义务来做，希望通过他们的黑客行为来警告一些网络或者系统漏洞，以达到警示别人的目的，因此，他们的行为没有丝毫恶意。

黑帽黑客是指那些专门研究病毒木马、操作系统、寻找漏洞，并且以个人意志为出发点，攻击网络或者计算机的人，已被认为是一个犯罪和黑客的混成语。

1.1.3 黑客基础知识

想要成为黑客并不是一件简单的事情，不仅要熟练掌握英文，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. 熟练掌握英文

黑客学习的计算机知识虽然主要来源于国内，但是却经常需要参考国外的相关资料和教程，而国外的资料和教程大多数为英文版本，因此就需要掌握一定的英文语言技能，以确保能够看懂国外的一些参考资料。

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、挂马和后门等词语，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 等命令，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等。

4. 掌握主流的编程语言及脚本语言

从互联网中获取的黑客工具通常是其他黑客利用指定类别的编程语言（C++、JAVA 等）制作的，如果想要成为一名黑客高手，仅仅使用别人制作的工具是不够的，需要自己具有独立的思想，通过掌握主流的 C++和 JAVA 等编程语言来创建属于自己的黑客工具。同时还需要掌握 JavaScript、VBScript 等脚本语言，用于自己编写脚本。

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、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，一般用于网页服务器。

（3）Hybrid Laguages（混合型语言）

代表是 JAVA 和 C#，介于解释型和编译型之间。

（4）COMPILING Languages（编译型语言）

C/C++和 JAVA 都是编译型语言。

（5）Assembly Languages（汇编语言）

汇编语言是最接近于硬件的语言，不过现在很少有人使用。

1.1.4 黑客常用术语

1. 肉鸡

“肉鸡”是一种很形象的比喻，比喻那些被黑客控制的电脑，对方可以是 Windows 系统，也可以是 UNIX/LINUX 系统，可以是普通的个人电脑，也可以是大型的服务器，一旦你的电脑成为“肉鸡”，就意味着别人可以随心所欲地操作你的电脑，而不会被你发觉。

2. 木马

就是那些表面上伪装成正常的程序，但是当这些程序运行时，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电脑，比如灰鸽子、黑洞、PcShare 等。

3. 网页木马

表面上伪装成普通的网页文件或将自己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的木马服务端下载到访问者的电脑上来自动执行。

4. 挂马

就是在别人的网站文件里面放入网页木马或者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

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，或者是修改某些设置。这些改动表面上很难被察觉，但是黑客却可以使用相应的程序或者方法来轻易地与这台电脑建立连接，重新控制这台电脑，就好象是客人偷偷地配了一把主人房间的钥匙，可以随时进出主人的房间而不被主人发现一样。通常大多数的特洛伊木马（Trojan Horse）程序都可以被黑客用于制作后门（BackDoor）。