


黑客攻防实战

从入门到精通 第2版

风云工作室 编著

网络安全常备手册

内容丰富：除讲解有线端的攻防策略外，还融入了无线攻防、移动端攻防、手机钱包等热点。
图文并茂：注重操作、图文并茂，在讲解案例的过程中，每一步操作均有对应的插图。
案例丰富：把知识点融入系统的案例实训当中，并且结合经典案例进行讲解和拓展。
超值赠送：赠送大量实用资源，可以全面掌握黑客攻防的方方面面知识。

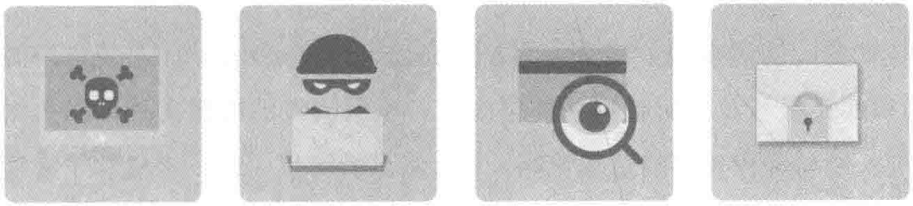



超值赠送：

- 950分钟实战教学视频
- 精美教学用的幻灯片
- 108个黑客工具速查手册
- 160个常用黑客命令速查手册
- 180页常见故障维修手册
- 188页Windows 10系统使用和防护技巧



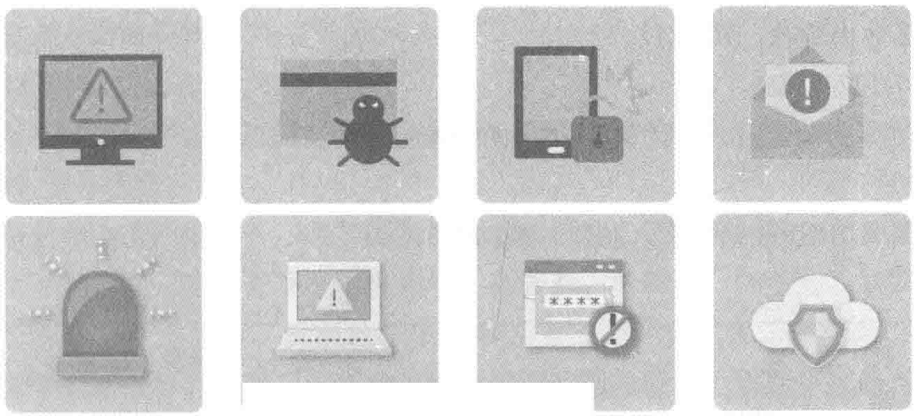
化学工业出版社



黑客攻防实战

从入门到精通 第2版

风云工作室 编著



化学工业出版社
·北京·

本书采用通俗易懂的语言，对读者进行黑客防御时迫切需要和想要用到的技术进行了详细的讲解，使读者对网络防御技术形成系统了解，从而能够更好地防范黑客的攻击。

全书共分为18章，包括熟悉黑客和红客，防黑必备技能大放送，防范黑客入侵的工具，系统漏洞与安全的防黑实战，电脑木马的防黑实战，Windows 10系统账户的防黑实战，网游、QQ和邮箱账号及密码数据的防黑实战，电脑病毒的防黑实战，网页浏览器的防黑实战，系统入侵与远程控制的防黑策略，U盘病毒的防黑实战，手机和平板病毒防范与清除，网站安全的防黑策略，磁盘数据安全的终极防黑实战，虚拟专用网的防黑实战，局域网的防黑实战，无线网络安全的防黑实战，手机钱包的防黑实战等内容。

本书内容丰富、图文并茂、深入浅出，不仅适合广大网络爱好者使用，也同样适合网络安全从业人员及网络管理员阅读。

图书在版编目(CIP)数据

黑客攻防实战从入门到精通/风云工作室编著. —2版.
—北京：化学工业出版社，2018.11
ISBN 978-7-122-32938-7
Ⅰ.①黑… Ⅱ.①风… Ⅲ. ①计算机网络-网络安全
Ⅳ.①TP393.08
中国版本图书馆CIP数据核字（2018）第200921号

责任编辑：孙　炜　李　辰　　装帧设计：尹琳琳
责任校对：边　涛

出版发行：化学工业出版社（北京市东城区青年湖南街13号　邮政编码100011）
印　　刷：三河市航远印刷有限公司
装　　订：三河市瞰发装订厂
787mm×1092mm　1/16　印张20　字数500千字　2019年1月北京第2版第1次印刷

购书咨询：010-64518888　　售后服务：010-64518899
网　　址：http：//www.cip.com.cn
凡购买本书，如有缺损质量问题，本社销售中心负责调换。

定　价：59.80元

Preface 前言

随着手机、平板电脑的普及，无线网络的防范就变得尤为重要，为此本书除了讲解有线端的攻防策略外，还把目前流行的无线攻防、移动端攻防、手机钱包防黑等热点融入本书中。

（1）本书特色

①知识点丰富、全面：本书涵盖了绝大多数黑客攻防知识点，由浅入深地讲解黑客攻防方面的技能。

②图文并茂：注重操作，图文并茂。在介绍案例的过程中，每一步操作都配有对应的插图。这种图文结合的方式使读者能够直观、清晰地看到操作的过程以及最终效果，便于更快地理解和掌握。

③案例丰富：把知识点融入系统的案例实训当中，并且结合经典案例进行讲解和拓展，进而达到“知其然，并知其所以然”的效果。

④提示技巧、贴心周到：本书对读者在学习过程中可能会遇到的疑难问题以“提示”的形式进行了说明，避免读者在学习的过程中走弯路。

⑤超值赠送：本书赠送了大量实用的资源，读者可以通过本书以及赠送的资源，掌握黑客攻防方方面面的知识。

（2）读者对象

本书不仅适合广大网络爱好者，而且适合网络安全从业人员及网络管理员阅读。

（3）写作团队

本书主要由王维维编著，参与编著的还包括王猛、王婷婷、张芳、王英英、张桐嘉、肖品、胡同夫、梁云亮、王攀登、包慧利、孙若淞、贺盼盼、郑玉超、唐跃爱、郭红侠、贺金刚、郭红梅、郑思贤、贾福运、贺单单、王二帅、郭红民、邓爱玲、谢德胜、李友洪、贾文学、郭推等。在编写过程中，笔者尽所能地将最好的讲解呈现给读者，但也难免有疏漏和不妥之处，敬请不吝指正。若您在学习中遇到困难或疑问，或有何建议，可加入QQ群389543972，获得作者的在线指导。

编著者

2018.3

Contents

目 录

第1章　熟悉黑客和红客

黑客（hacker）最初是指那些热衷于电脑，并能够把一些应用程序组合起来或拆开来解决问题的人；但如今，黑客被定义为非法搜索和渗透计算机网络访问和使用数据的人。黑客之所以存在的原因主要是由于系统、网络和软件在一定程度上都存在有安全漏洞，黑客就是利用这些漏洞来攻击目标主机的。

1.1　黑客的过去、现在和未来

随着Internet的迅速发展、网络带宽的快速提升、网络用户群体的增加，网络的安全问题也变得越来越突出。网络攻击的便利性和简易性以及我国网络信息系统的安全脆弱性，进而导致了黑客攻击的多发性。

1.1.1　黑客的发展历史

随着Internet在中国迅速发展、国内上网的人数的持续翻番以及网民的日益活跃，“黑客”事件也时有发生。国内黑客发展主要经历如下3个阶段：

①第1代（1996～1998年）。1996年因特网在中国兴起，但是由于受到各种条件的制约，很多人根本没有机会接触网络。当时计算机也没有达到普及的程度，大部分地区还没有开通因特网的接入服务，所以中国第1代黑客大都是从事科研、机械等方面工作的人，只有他们才有机会频繁地接触计算机和网络。他们有着较高的文化素质和计算机技术水平，凭着扎实的技术和对网络的热爱迅速发展成为黑客。有的专门从事网络安全技术研究或成为网络安全管理员，有的则开了网络安全公司，演变为派客（由黑客转变为网络安全者）。

1998年8月爆发了东南亚金融危机，并且在一些地区发生了严重的针对华人的暴乱，当时残害华人的消息在新闻媒体上报道后，国内计算机爱好者怀着一片爱国之心和对同胞惨遭杀害的悲痛之心，纷纷对这些行为进行抗议。中国黑客对这些地区的网站发动了攻击，众多网站上悬挂起中华人民共和国的五星红旗。当时黑客代表组织为“绿色兵团”。

②第2代（1998～2000年）。随着计算机的普及和因特网的发展，有越来越多的人有机会接触计算机和网络，在第1代黑客的影响和指点下，中国出现了第2代黑客。他们一部分是从事计算机的工作者和网络爱好者，另一部分是在校学生。这一代的兴起是由1999年5月8日某国轰炸驻中国南斯拉夫大使馆事件引发，黑客代表组织为原“中国黑客联盟”。

③第3代（2000年～）。这一代黑客主要由在校学生组成，其技术水平和文化素质与第1代、第2代相差甚远，大都只是照搬网上一些由前人总结出来的经验和攻击手法。现在网络上所谓的入侵者也是由这一代组成。但领导这一代的核心黑客还是那些第1代、第2代的前辈们。这一代兴起是由2001年4月的一起撞机事件引发，黑客代表组织为“红客联盟”“中国鹰派”。

1.1.2　黑客的现状以及发展

国内黑客站点门派繁多，但整体素质

不尽如人意，有的甚至低劣。主要表现在如下6方面：

（1）叫法不一，很不正规

黑客，甚至包括骇客，这两个单词都是可以在相关资料如词典、黑客界等领域有章可循的。目前的对“黑客”一词的各种叫法极不规范。

（2）技术功底薄弱，夸大作风

比如国内几大黑客组织的站点，此类站点只顾如何叫他人攻击别人的电脑，刷Q币，盗密码等，以适应初学者的口味。站点用色彩绚丽的界面和震撼的音乐等手段，来吸引众人尤其是青少年的眼球。青少年不成熟，崇尚自由冒险刺激，有强烈的表现欲，黑客行业正符合这一特点，所以众多黑客站点正投其所好，使之趋之若鹜，来提高自己的站点访问量，而不用靠实力提高站点的质量和知名度。

（3）内容粗制滥造

内容粗制滥造，应付了事，原创作品少，且相互抄袭。曾有某篇文章说，中国的黑客一代不如一代。

（4）效率低，更新少，可读性差，界面杂乱

有些站点很少更新，打不开，站点杂乱，经常有死链接，作品抄袭。

（5）整体技术水平不高，研究层次级别低

目前国内几大黑客站点大都进行商业化运作，安全培训。以追求最大经济效益为目的，只要能赚到钱就够了，至于深层次的研究，是没有的。只是每天更新一些新闻、黑客教程、软件等，用户只能学到一些编程知识、数据库知识，再看看一些教程，借用一些黑客工具，就去黑别人的站点，盗号等。与国外相比，国外的黑客研究的则是系统级别的漏洞，制造的也是世界级别的系统病毒，扰乱全球网络。

（6）缺少一个统一协调中国黑客界行动发展的组织

虽然目前好多站点都包含有“联盟”字样，但其实是一家，各自为政，这就使得在抗击外来网络入侵时缺少统一指挥，手忙脚乱，大大降低中国黑客界整体的力量。

目前中国黑客的发展总体可以归为5大趋势：

①黑客年轻化。由于中国互联网的普及，形成全球一体化，甚至连很多偏远的地方也可以从网络上接触到世界各地的信息资源，所以越来越多对这方面感兴趣的中学生，也已经踏足到这个领域。

②黑客的破坏力扩大化。由于互联网的普及，电子商务也在蓬勃发展，全社会对互联网的依赖性日益增加，黑客的破坏力也日益扩大化。仅在美国，黑客每年造成的经济损失就超过100亿美元，可想而知，对于安全刚起步的中国，破坏的影响程度就更大了。

③黑客技术的迅速普及。黑客组织的形成和黑客傻瓜式工具的大量出现导致的一个直接后果就是黑客技术的普及，虽然在市面可能看不到一本介绍如何做黑客、传授黑客技术的书，但是在Internet上，黑客与黑客组织办的传授黑客技术的站点却比比皆是。

④黑客技术的工具化。黑客事件越来越多的一个的重要原因，是黑客工具越来越多，越来越容易获得，也越来越傻瓜化和自动化，目前黑客运用的软件工具已超过1000种。

⑤黑客组织化。对于黑客的破坏，人们的网络安全意识开始增强，计算机产品的安全性被放在很重要的位置，漏洞和缺陷也越来越难发现；而且因为利益的驱

使，黑客开始由原来的单兵作战变成了有组织的黑客群体。在黑客组织内部，成员之间相互交流技术经验，共同采取黑客行动，成功率增高，影响力也更大，正所谓“道高一尺，魔高一丈”。

1.1.3　哪些是黑客做下的“事”

黑客利用扫描出来的目标主机漏洞主要做如下事情：首先是获得系统信息，有些系统漏洞可以泄漏系统信息，暴露敏感资料，为进一步入侵系统做好准备；其次是入侵系统，通过漏洞进入系统内部，从而取得服务器上的内部资料。

下面介绍一些历史上比较著名的黑客事件，从而进一步帮助读者了解黑客。

1983年，凯文·米特尼克因被发现使用一台大学里的电脑擅自进入今日互联网的前身ARPA网，并通过该网进入了美国五角大楼的电脑。

1999年，梅利莎病毒使世界上300多家公司的电脑系统崩溃，该病毒造成的损失接近4亿美元，它是首个具有全球破坏力的病毒。

2000年，绰号“黑手党男孩”的黑客在2000年2月6日到2月14日情人节期间成功侵入包括雅虎、eBay和Amazon在内的大型网站服务器，他成功阻止服务器向用户提供服务。

2008年，一个全球性的黑客组织，利用ATM欺诈程序在一夜之间从世界49个城市的银行中盗走了900万美元。黑客们攻破的是一种名为RBS WorldPay的银行系统，并在11月8日午夜，利用团伙作案从世界49个城市总计超过130台ATM机上提取了900万美元。

2009年7月7日，黑客对韩国总统府、国会和国防部等国家机关，以及金融界、媒体和防火墙企业网站进行了攻击。9日韩国国家情报院和国民银行网站无法被访问，韩国国会、国防部等机构的网站一度无法打开，这是韩国遭遇的有史以来最强的一次黑客攻击。

2010年1月12日上午7点钟开始，全球最大中文搜索引擎“百度”遭到黑客攻击，长时间无法正常访问，主要表现为跳转到雅虎出错页面、出现“天外符号”等，范围涉及四川、福建、江苏、吉林、浙江、北京、广东等国内绝大部分省市，这是自百度建立以来，所遭遇的持续时间最长、影响最严重的黑客攻击。

这些事件的发生，表明黑客渐趋于普遍化。计算机网络安全问题关系到国家的安全，关系到国家经济秩序的稳定，也关系到自由通信会不会受到来路不明的黑客袭击或干扰。

1.2　黑客与红客的区别

“黑客”大体上可以分为“正”“邪”两类，正派黑客依靠自己掌握的知识帮助系统管理员找出系统中的漏洞并加以完善；而邪派黑客则是通过各种黑客技能对系统进行攻击、入侵或做其他一些有害于网络的事情，正是因为邪派黑客所从事的事情违背了《黑客守则》，所以他们真正的名字应该叫“骇客”（Cracker）而非“黑客”（Hacker），这也就是平时经常听说的“黑客”（Cacker）和“红客”（Hacker）。

不管是“黑客”或者是“红客”，他们最初的学习内容和掌握的基本技能都是一样的，即便日后他们各自走上了不同的道路，但是所做的事情也差不多，只不过出发点和目的不一样而已。

知识链接

什么是黑客守则

目前，网络上总结出来的黑客守则有很多，主要包括以下几个方面。

①不得恶意破坏任何的系统。

②不得恶意修改任何系统文件。

③不要轻易将要攻击的网站告诉不信任的朋友。

④不要在论坛上谈论关于攻击的任何事情。

⑤正在入侵的时候，不要随意离开电脑。

⑥不要侵入或破坏政府机关的主机。

⑦将黑客笔记放在安全的地方。

⑧已侵入电脑中的账号不得清除或涂改。

⑨不得恶意修改系统档案。

⑩不将已破解的账号与朋友分享。

1.3 防范黑客需要掌握的资源

一般来讲，做什么事情都是入门难。要想防范黑客的进攻，就需要了解黑客都需要掌握哪些知识，其实也是一个不断学习的过程，那么比较简便的方法就是借助网络和书籍。比较常见的书籍有以下几种类型

①基础知识类。一般来说新手朋友的基础是比较差的，甚至一些基本常识都不知道，所以有几本基础知识的书作为参考是必不可少的，比如关于TCP/IP、网络、操作系统以及局域网等，甚至是关于DOS、Windows基础的书都是很有必要的。此类书籍关键在于它的通俗易懂性，不要追求多么深入，对新手来说，急于求成是最要不得的。

②大众杂志类。此类书籍的精华在于其合订本，比如电脑报合订本、电脑应用合订本等，就相当于一个大百科，具有分类详细、内容丰富的特点。此类书籍的优势在于内容全面，各个方面都能涉及，查找方便，但因其定位在大众杂志，内容相对比较基础，适合新手做全方位了解。

③hack杂志类。比如《黑客防线》《黑客X档案》《黑客手册》等，此类杂志专业性强，内容由浅入深，讨论详细，并附送光盘，对比较富裕的朋友来说是个不错的选择。这是一种比较好的入门方法。

④查看电子教程。在网络中搜索查看电子教程是能让自己快速进步的方法之一，如到各大安全站点的文章系统中去找，或者去相关论坛或Google中去搜索。

1.4 防患于未然——黑客是如何攻击电脑的

黑客攻击电脑的方式是多种多样的，绝大多数攻击是利用系统配置的缺陷、操作系统的安全漏洞以及通信协议的安全漏洞等进行攻击的。目前，黑客攻击的主要方式有以下几种：

（1）拒绝服务攻击

在一般情况下，拒绝服务攻击是通过使被攻击对象（工作站或重要服务器）的系统关键资源过载，从而使被攻击对象停止部分或全部服务。目前拒绝服务攻击是最基本的入侵攻击手段，也是最难对付的黑客攻击之一，SYN Flood攻击、Ping