HACKER
ATTACK AND DEFENSE

黑客攻防从入门到精通

实战秘笈版

九天科技◎编著

知识丰富　图文并茂　案例丰富

- 涵盖了黑客攻防知识点，PC端的攻防策略、无线攻防、移动端攻防、手机钱包等内容
- 注重操作，图文并茂，在介绍案例的过程中，每一个操作均有对应的图片示例
- 把知识点融于系统的案例实训中，结合经典案例进行讲解和拓展

微信扫一扫 轻松看视频

书中关键知识点视频演示，不仅可在PC端播放，还可随时在手机端观看，实现即扫即看

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

黑客攻防从入门到精通

九天科技◎编著

实战秘笈版

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

本书从黑客“攻”、“防”两个不同的角度出发，深入介绍了黑客经常使用的入侵手段和工具，以及防御黑客攻击所必须掌握的方法、工具和技巧等知识。本书共分为 12 章，主要内容包括：黑客攻防入门必修，构建虚拟测试环境，黑客常用的 DOS 命令，黑客攻击目标的扫描与嗅探，远程入侵与控制黑客攻防实战，系统漏洞黑客攻防实战，系统安全黑客攻防实战，账户与密码黑客攻防实战，QQ 与电子邮件黑客攻防实战，木马与病毒黑客攻防实战，无线网络及智能手机安全防御，以及网络支付安全防御实战。

本书适合想了解并掌握黑客攻防技术的初学者，以及对黑客攻防与网络安全维护感兴趣的读者学习使用，也可作为 IT 从业人员、网络安全从业人员及网络管理员的参考用书。

图书在版编目（CIP）数据

黑客攻防从入门到精通：实战秘笈版/九天科技编著. —北京：中国铁道出版社，2017.9

ISBN 978-7-113-23320-4

Ⅰ.①黑… Ⅱ.①九… Ⅲ.①黑客—网络防御 Ⅳ.①TP393.081

中国版本图书馆 CIP 数据核字（2017）第 142721 号

书　　名：黑客攻防从入门到精通（实战秘笈版）
作　　者：九天科技　编著

策　　划：苏　茜　　**读者热线电话**：010-63560056
责任编辑：张　丹
责任印制：赵星辰　　**封面设计**：MX DESIGN STUDIO

出版发行：中国铁道出版社（北京市西城区右安门西街 8 号　　邮政编码：100054）
印　　刷：北京鑫正大印刷有限公司
版　　次：2017 年 9 月第 1 版　　2017 年 9 月第 1 次印刷
开　　本：787mm×1092mm　1/16　　**印张**：18.75　　**字数**：597 千
书　　号：ISBN 978-7-113-23320-4
定　　价：49.80 元

前 言 PREFACE

目前网上支付、购物、投资、理财等已经成为人们日常消费生活的重要内容，财产的安全性也越来越受到人们的关注。如果账户、密码被黑客截取，将会带来非常大的经济损失。因此黑客攻击已经成为威胁网络安全的重大隐患之一。随着网络的大范围普及、黑客工具的迅速传播，黑客只需使用简单的工具就能对一些疏于防范的电脑或移动终端进行攻击，并在受侵的电脑或终端中为所欲为。当发现自己的密码被盗、资料被修改或删除、硬盘变成一片空白时再想进行补救，为时已晚。

虽然黑客的攻击手段越来越“高明”，但防御黑客攻击的方法也在不断增强，如果您对黑客攻击和防御还比较陌生，还不了解常用黑客工具的使用方法，对木马程序和远程监控一无所知，不懂无线网络、智能手机与网络支付安全防御，并且经常受到电脑病毒和木马的侵袭，等等。那么请您静下心来阅读本书，它将带您进入变幻莫测的黑客世界。

内容导读

本书旨在帮助读者清晰地了解黑客入侵的攻击方式，进而制订出完善的防御方案，同时从另一个完全不同的角度全面解读黑客攻防，深入洞察防御的死角，组织更为严密的防御体系，以应对层出不穷的黑客入侵挑战。

主要特色

本书由业内资深信息安全专家精心策划编写，其主要特色如下：

- **从零开始，无师自通**

无论您是否在从事电脑行业工作，无论您是否接触过网络，无论您以前是否了解黑客攻防技术，都能从本书中找到适合自己的起始点，开启黑客攻防的学习历程。

- **侧重实战，案例演绎**

本书侧重实战技能，摒弃晦涩难懂的技术理论，基于实际案例的分析和操作指导，让读者学习起来更加轻松，操作起来有章可循。

- **图文并茂，易学易用**

采用图文结合的方式使读者在学习过程中能够直观、清晰地看到案例操作的过程及效果，以便更快速地理解和掌握。颠覆“看”书的传统观念，变成一本能“操作”、能“上手”的图书。

- **传授经验，私房秘笈**

在本书中穿插了大量黑客攻防提示与技巧，且在每章最后均设有“高手私房秘笈”版块，真正帮助读者解决在学习和工作中遇到的各种难题。

视听视频，模拟课堂

为了增加读者的学习渠道，增强读者的学习兴趣，本书配有超大容量多媒体视听教学视频，读者可以跟着其提供的语音视频进行实战演练，并能快速应用于实际工作中。

视频说明

本书随书配有交互式、600 分钟超长播放的多媒体视听教学视频，它是与图书完美结合的视听课堂，让您像看电视一样轻松、直观地进行学习。

如何获取视频教程：

1. “扫一扫”封面上的二维码，在打开的界面上单击本书所对应的下载文件；
2. 选择保存路径后开始下载；

备注：读者只需解压一个文件，即可免费得到全部视频内容。

视频下载地址：http://www.crphdm.com/2017/0620/13570.shtml

微信扫一扫
轻松看视频

视频中超值赠送由本社出版的《全图解电脑软硬件维修实用大全》和《全图解电脑组装与维修实用大全》的视频教程，超大容量，物超所值。

适用读者

本书适用面广，适合以下读者学习使用：

（1）没有任何电脑黑客攻防知识的初学者；
（2）对电脑黑客攻防技术有些了解但不精通的学习者；
（3）网络安全从业人员以及网络管理员；
（4）大、中专院校的在校学生和社会电脑安全培训机构的学员；
（5）想在短时间内掌握电脑安全实用技能的读者朋友。

售后服务

如果读者在使用本书的过程中遇到问题或者有好的意见或建议，可以通过发送电子邮件（E-mail：9335404@qq.com）或者在线 QQ：843688388 联系我们，我们将及时予以回复，并尽最大努力提供学习上的指导与帮助。

特别提醒：

根据国家有关法律规定，任何入侵和窃取他人系统和文件的做法都是违法的，希望读者不要使用本书介绍的黑客技术攻击他人电脑，否则后果自负，特此声明！

编　者

2017 年 5 月

第 1 章 黑客攻防入门必修

高手私房秘笈

第 2 章 构建虚拟测试环境

高手私房秘笈

第 3 章 黑客常用的 DOS 命令

高手私房秘笈

第 4 章 黑客攻击目标的扫描与嗅探

高手私房秘笈

秘笈 1　设置 QQ 邮箱独立密码
秘笈 2　加密邮件

第 10 章 木马与病毒黑客攻防实战

第 11 章 无线网络及智能手机安全防御

第 12 章 网络支付安全防御实战

高手私房秘笈

以下拓展内容，请扫描二维码阅读 PDF 文件

扫一扫，看 PDF 文件

附录 A 系统的备份与还原

附录 B 网页恶意代码黑客攻防实战

附录 C U 盘病毒黑客攻防实战

第1章 黑客攻防入门必修

互联网改变了人们的生活，但黑客问题也成为全世界的关注热点。在学习黑客攻防之前，首先了解一些关于黑客的基础知识，认识黑客、网络协议、端口，以及系统进程等。

|内|容|导|航|

- 黑客揭秘
- 认识网络协议
- 黑客攻击的入口——端口
- 木马藏匿的首选地——系统进程

视频链接

本章知识相关的多媒体教学视频，请读者参见“教学视频\第 1 章”。

1.1 黑客揭秘

谈到网络安全，人们不自觉就会联想到黑客，人们往往会将他们同破坏网络安全、盗取用户账号、偷窃个人私密信息联系起来。其实黑客也有好坏之分，他们并不全是网络上的捣乱分子，其中也有一部分是网络上的安全卫士。下面就让我们揭开黑客的神秘面纱，让读者详细了解黑客到底是什么样的群体。

在黑客圈中，Hacker 一词早期是带有正面意义的。但到了今天，“黑客”一词已经被用于那些专门利用电脑进行破坏或入侵他人电脑者系统的人的代言词，其实对这些人正确的叫法应该是 Cracker，也有翻译成“骇客”。也正是由于这些人的出现玷污了“黑客”一词，使人们把黑客和骇客混为一谈。黑客和骇客根本的区别是：黑客修补系统漏洞，而骇客利用系统漏洞进行破坏。

1.1.1 黑客的由来

黑客始于 20 世纪 50 年代，最早的电脑是 1946 年在宾夕法尼亚大学出现，最早的黑客出现于麻省理工学院、贝尔实验室也有。最初的黑客一般都是一些高级技术人员，他们热衷于挑战、崇尚自由，并主张信息共享。

1994 年以来，互联网在全球的迅猛发展为人们提供了方便、自由和无限财富，政治、军事、经济、科技、教育、文化等各个方面都越来越网络化，并且逐渐成为人们生活、娱乐的一部分。可以说，信息时代的到来，使信息已成为物质和能量以外维持人类社会的第三大资源，是未来生活中的重要介质。随着电脑的普及和互联网技术的迅猛发展，黑客也随之出现。

“黑客”一词一般有以下 4 种意义：

- 一个对（某领域内的）编程语言有足够了解，可以不用经过长时间思考就能创造出有用软件的人。
- 一个试图恶意（一般是非法地）破解或破坏某个程序、系统及网络安全的人。这个意义经常对那些符合上个条件的黑客造成严重困扰，他们建议媒体将这群人称为“骇客”。
- 一个试图破解某系统，以提醒该系统所有者系统存在安全漏洞，这群人往往被称作“红客”。他们大多数是电脑安全公司的雇员，并且在完全合法的前提下攻击某系统。
- 一个通过知识或猜测而对某段程序做出（往往是好的）修改，并改变（或增强）该程序用途的人。

现在，网络上出现了越来越多的 Cracker，他们只会入侵，使用扫描器到处乱扫，用 IP 炸弹轰炸，毫无目的地入侵、破坏，他们并无益于电脑技术的发展，反而有害于网络的安全，甚至造成网络瘫痪，为人们带来巨大的经济和精神损失。

1.1.2 黑客的组成

今天，黑客不再像以前那样神秘，他们已经发展成网络上一个独特的群体。他们有着与常人不同的思维方法，有着自己独特的行为模式，网络上现在出现了很多由志同道合的人组织起来的黑客组织。但这些人是从什么地方来的呢？他们是什么样的人？其实除了极少数的

职业黑客以外，大多数都是业余的，而黑客其实和现实中的平常人没有两样，或许他就是一名普通的高中生。

有人曾经对黑客年龄进行过调查，黑客的主要群体是18~30岁之间的年轻人，大多数是男性，不过现在也有很多女性加入这个行列。他们大多数是在校学生，爱好电脑、充足的时间、好奇心强、精力旺盛等使他们步入黑客的行列。还有一些黑客有自己的事业或工作，大致分为程序员、资深安全员、安全研究员、职业间谍、安全顾问等。当然，这些人的技术和水平是刚刚入门的“小黑客”无法比拟的，不过他们也是从这里一点点地走过来的。

1.1.3 黑客的主要行为

“黑客”大体上分为“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、入侵或者做一些其他有害于网络的事情。

无论哪类黑客，他们最初的学习内容都是本书所涉及的内容，而且掌握的基本技能也都是一样的。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。

黑客的行为主要有以下几种。

其一，学习技术。互联网上的新技术一旦出现，黑客就必须立刻学习，并用最短的时间掌握这项技术。这里所说的掌握并不是一般的了解，而是阅读有关的“协议”、深入了解此技术的原理。否则一旦停止学习，仅依靠他以前掌握的内容，也许都不能维持他的“黑客”身份超过一年。

其二，伪装自己。黑客的一举一动都会被服务器记录下来，所以黑客会伪装自己，使得对方无法辨别其真实身份。这需要有熟练的技巧，包括伪装自己的IP地址、使用跳板逃避跟踪、清理记录扰乱对方线索、巧妙躲开防火墙等。

伪装是需要非常过硬的基本功才能实现的，初学者不可能在短时间内学会伪装，本书并不鼓励读者利用自己学习的知识对网络进行攻击，否则一旦自己的行迹败露，最终害的还是自己。

其三，发现漏洞。漏洞对黑客来说是最重要的信息，黑客要经常学习别人发现的漏洞，并努力自己寻找未知漏洞，从海量的漏洞中寻找有价值的、可被利用的漏洞进行试验。当然，他们最终的目的是通过漏洞进行破坏或者修补上这个漏洞。

其四，利用漏洞。对于正派黑客来说，漏洞需要被修补；对于邪派黑客来说，漏洞主要是用来搞破坏。

作为一名黑客，道德是非常重要的，这往往决定一个黑客的前途和命运。如果一名黑客在开始学习时就是为了扬名或非法获利，那就不能称之为黑客。但是，虚拟的网络世界不能用现实中的规范去管理，而黑客又是在这个虚拟世界中最渴望自由和共享的。虽然网络上的黑客道德或规则出现很多，也有很多黑客章程，但这些所谓的道德往往只是一纸空文，而黑客们真正遵守的是来自内心真诚的道德，是一种信仰而不是人为的、外在的一种守则。也只有这些来自于黑客内心中的道德才可以真正地约束他们。

现在有不少人以盗取他人的游戏账号、银行卡号、窃取公司机密、攻击别人网站、敲诈、

欺骗等非法获利，这些都是违法行为，这些人都不能称为“黑客”，应该称为“骇客”更为合适，他们最终会受到法律的严惩。

1.1.4 黑客术语

1. 肉鸡

“肉鸡”是一种很形象的比喻，比喻那些可以被黑客控制的电脑，对方可以是 Windows 系统，也可以是 UNIX/Linux 系统，可以是个人电脑，也可以是大型的服务器，黑客可以像操作自己的电脑那样来操作“肉鸡”，而不被对方发觉。

2. 木马

木马程序表面上伪装成正常的程序，一旦被用户运行，就会获取系统的控制权限。有很多黑客热衷于使用木马程序来控制他人的电脑，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是将黑客代码直接插入正常的网页文件中，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并自动执行。

4. 挂马

在别人的网站中放入网页木马，或是将黑客代码潜入对方正常的网页中，以使浏览者中木马病毒。

5. 后门

后门是一种很形象的比喻，入侵者在利用某些方法成功地控制目的主机后，可以在对方的系统中植入特定的程序，或者修改某些设置。这些改动从表面上很难被察觉，但是入侵者却可以使用相应的程序或者方法轻易地与这台电脑建立连接，重新进行控制。这就好像是入侵者偷偷地配了一把主人房间的钥匙，可以随时进出而不被主人发现一样。通常大多数的木马程序都可以被黑客用于制作后门。

6. 端口

端口（Port）相当于一种数据的传输通道。用于接受某些数据，然后传输给相应的服务。电脑将这些数据处理后，再将相应的回复通过开启的端口传给对方。一般每一个开放的端口对应了相应的服务，要关闭这些端口只需要将对应的服务禁用即可。

7. rootkit

rootkit 中 root 术语来自于 UNIX 领域，由于 UNIX 主机系统管理员账号为 root 账号，该账号拥有最小的安全限制，完全控制主机并拥有管理员权限称为“root”了这台电脑。rootkit 是攻击者用来隐藏自己的行踪和保留 root（根权限，可以理解成 Windows 下的 system 或者管理员权限）访问权限的工具。攻击者通过远程攻击的方式获得 root 访问权限，或者是先使用密码猜解的方式获得对系统的普通访问权限，进入系统后，通过对方系统内存在的安全漏洞获得系统的 root 权限。然后，攻击者就会在对方的系统中安装 rootkit，以达到自己长久控制对方系统的目的。rootkit 与木马和后门很类似，但远比木马、后门要隐蔽。简单地说，rootkit