The Introduction and Practice Detailed Annotation of Hacking and Defence

黑客攻防入门与实战详解

至诚文化 编著

知己知彼，百战不殆

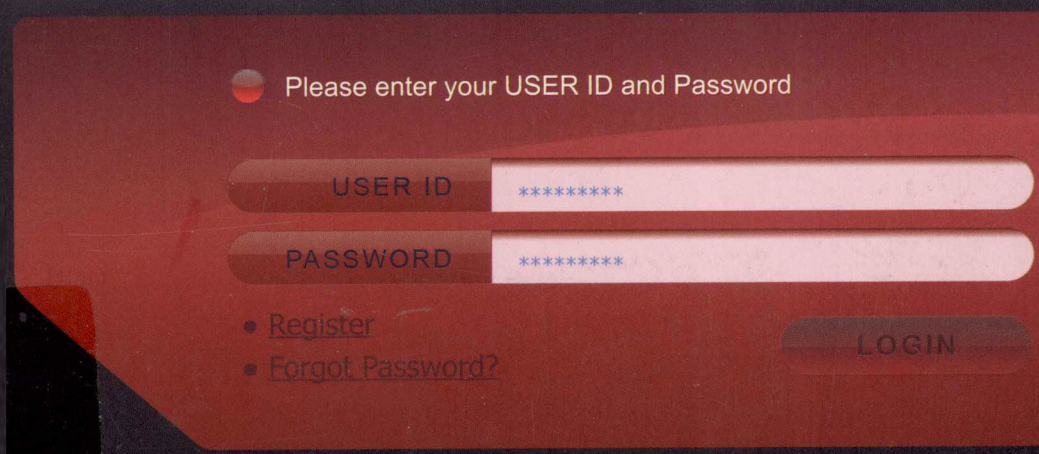
秉承保障网络安全的原则，夯实黑客基础知识，全面呈现当前黑客攻防的各类实用技巧和经典案例。

more

大容量多媒体视频

精心筛选各类实用技巧和经典真实案例，分门别类地详细阐述，力求通过直观影像帮助读者轻松掌握。

more



中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

黑客攻防入门与实战详解

至诚文化　编著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

本书秉承“知己知彼”的理念，详细阐述了在网络安全的具体实践中所用到的各类原理、技巧和工具，例如：了解黑客、命令行、端口扫描、漏洞扫描、网络嗅探、局域网干扰防御、木马攻防、痕迹清除与加密破解等，旨在帮助读者清晰地了解入侵者的攻击方式，进而能制作出完善的防御方案，同时从另一个完全不同的角度全面解读系统安全，从而洞察防御的死角，组织更为严密防御体系以应对层出不穷的入侵挑战。

图书在版编目（CIP）数据

黑客攻防入门与实战详解/至诚文化编著. --北京：中国铁道出版社，2011.9

ISBN 978-7-113-13243-9

Ⅰ.①黑… Ⅱ. ①至… 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（2011）第 133948 号

书　　名：黑客攻防入门与实战详解
作　　者：至诚文化　编著

责任编辑：荆　波　　**读者热线电话：**010-63560056
特邀编辑：李新承
封面设计：付　巍　　**封面制作：**郑少云
版式设计：于　洋　　**责任印制：**李　佳

出版发行：中国铁道出版社（北京市宣武区右安门西街 8 号　　邮政编码：100054）
印　　刷：化学工业出版社印刷厂
版　　次：2011 年 9 月第 1 版　　2011 年 9 月第 1 次印刷
开　　本：787mm×1092mm　1/16　　**印张：**17.5　　**字数：**408 千
书　　号：ISBN 978-7-113-13243-9
定　　价：39.80 元（附赠光盘）

前　言　Foreword

在影视作品中，许多黑客入侵时都是满头大汗、弹指如飞，屏幕上的画面则不停闪烁。事实上，这是为了体现紧张气氛而特别渲染的情节。实际上的黑客入侵过程平平淡淡，就像处理普通公文，甚至像与朋友聊天一样简单。例如世界十大黑客之一的阿德里安·拉莫（Adrian Lamo），他就经常坐在大企业旁的咖啡店、图书馆等免费上网场所上网，然后运行他自己编写的入侵程序，一边休闲地品味着茶点，一边等待程序给出入侵结果。即使联邦密探就坐在他不远处喝咖啡，也很难发现他正在完成高难度的入侵行为。

而更让无数安全专家们头痛的事情是，不需要任何深厚的网络通信基础，也不需要深入了解操作系统，只要拥有相应的黑客程序，任何普通用户都可以摇身变成强悍的黑客。如何防御及应对这些问题是摆在眼前最急需解决的问题。

所谓“知己知彼，百战不殆”，要应对这类黑客入侵，最切实可行的方法就是了解广泛流传的各类黑客“兵器”，从它们的攻击特性着手，有的放矢进行针对性的拦截及防御。有鉴于此，本书从网络安全的各个领域入手，在精练地讲解基本知识与原理的同时更收录了众多著名黑客和黑客组织的“成名”作品，其内容涉及网络扫描、网络嗅探、局域网入侵、局域网干扰、网络欺骗和密码破解等多个方面，以供各位有志于研究黑客入侵的用户参考和学习。我们分析这些工具的目的只有一个：知己知彼，保障自己的数据安全。

第 1 章　走近黑客

几乎每一个网民都听过有关“黑客”的新闻或传闻。他们与 FBI 玩捉迷藏游戏，他们散布“熊猫烧香”为祸网络，他们打造价值百亿的木马病毒产业链疯狂敛财……翻开这一章，你将认识真正的黑客，纵观半个世纪黑客发展的足迹，了解黑客与程序之间的不解之缘，并洞悉黑客走过的捷径。

第 2 章　黑客与命令行

谈起黑客命令，很多人都会认为那是网络绝顶高手的杀手锏，利用它们可以监视网络中的一举一动，利用简单的几个字母即可拒敌于千里之外。其实黑客命令行是非常有用、针对性极强的网络安全维护工具。

第 3 章　端口扫描

端口扫描就相当于探子打探军情，它可以让黑客获得目标主机的一些信息，分析其可能存在的弱点。因此作为系统管理员，非常有必要了解端口扫描的相关知识，以便采取相应的防御措施。在这一章中，将学习端口扫描及防御扫描的技能。

第 4 章　漏洞扫描

任何一个系统都或多或少存在着漏洞。网络安全人员和黑客抢着不同的目的都在努力寻找漏洞，区别在于网络安全人员要发现并修复它，而黑客则是发现并利用它进行入侵。本章将从漏洞扫描的原理开始讲解，介绍黑客如何扫描主机，以及应对扫描侦测的防御手段。

第 5 章　网络嗅探

网络嗅探是一把双刃剑，黑客利用它刺探网络密码和即时通信消息内容，而网络管理员则用它监听网络并查找故障，是正是邪存乎一念之间。在这一章中，我们将摘除所有“有色眼镜”，从纯技术方面探讨网络嗅探的原理，学习网络嗅探软件的使用，以及摆脱网络嗅探的技能。

第 6 章　局域网干扰与防御

虽说“兔子不吃窝边草”，但出于各种利益目的，不少校园网、企业网及网吧都成为黑客们暗战不断的沙场。在这一章中，将会看到精彩的局域网攻防作战，尽览黑客 ARP 攻击、IP 冲突攻击、洪泛攻击和广播风暴等层出不穷的攻击手法，同时也会看到管理员如何见招拆招，将凶猛的攻击一一化解。

第 7 章　无线网络破解

随着无线网络器材的普及，不少家庭、企业等都使用了架设方便的无线局域网。但你是否想过，无形的电波在带来方便的同时，也带来了新的安全威胁？在这一章中，将学习黑客如何将黑手伸进受 WEP、WPA 加密保护的无线网络，并且找到防御应对入侵的办法。

第 8 章　本地入侵

将 U 盘插进对方计算机中，只需按几下键盘就将对方的商业机密偷走，那仅是电影幻想中的情节。事实上黑客即使能直接操作目标主机，可能也还需要面对 BIOS 开机密码、操作系统登录密码等“拦路虎”。在这一章中，将介绍黑客破除障碍登录本地计算机的手法，并学习如何严密设防自己的主机，以防私密或机密信息被盗。

第 9 章　网络远程控制

在这一章中，首先了解黑客如何利用正向连接控制、监视有公网 IP 的主机，以及穿透内网以反弹连接入侵内网主机。在掌握黑客的动向之后，将学习如何设置防火墙规则，阻断非法的黑客连接。

第 10 章　木马攻防

木马是网络上最普遍的安全威胁，不少用户都有过 QQ、网游账号被盗的经历，有的甚至连银行账号都被盗了。在这一章中，将介绍黑客如何利用木马为非作歹，而作为管理员又该如何防御网站挂马，以及保护个人计算机不被木马入侵。

第 11 章　跳板与痕迹清除

受聘于安全机构的白帽黑客可以合法地扫描系统漏洞，尝试入侵指定的计算机，但大多数隐藏于暗处的黑客却没有这个特权，即使出于技术研究目的，扫描或破解他人的系统，也可能会引来牢狱之灾。在这一章中，将介绍有经验的黑客如何清除入侵痕迹和利用网络跳板保护自己不被追踪发现，以帮助管理员了解黑客的手法，掌握如何追踪黑客的入侵痕迹。

第 12 章　加密破解

破解加密数据是黑客界长盛不衰的热点话题。在这一章中，首先将了解黑客如何破解各种常见的加密文件，然后站在更高的角度来研究如何强化文件加密，以保护自己的个人隐私和公司的商业机密。

我们真切地期望这本书能使读者从零起步，轻松体验黑客的典型攻击，涉猎更多的黑客攻防知识，从而打造出更安全、稳健的系统及网络。

光盘使用说明：

为保障数据安全，我们没有使用自动播放功能，读者可右击光盘标，单击“打开”命令，在打开的界面中双击“autorun.exe”即可进入多媒体界面。

编　者

2011 年 7 月

郑重声明

本书旨在通过“知己知彼，百战不殆”的方式帮助读者熟悉目前网络安全的危急形势，唤醒公众的网络安全常识，进而保护好自己的数据。绝不是为那些怀有不良动机的人提供技术支持，也不承担因技术被滥用所产生的连带责任。

目　录　Contents

第 1 章　走近黑客

第 2 章　黑客与命令行

第 6 章 局域网干扰与防御

第 9 章 网络远程控制

第 10 章 木马攻防

第 11 章　跳板与痕迹清除

第 12 章　加密破解

第1章 走近黑客

几乎每一个网民都听过有关“黑客”的新闻或传闻。他们与FBI玩捉迷藏游戏，他们散布“熊猫烧香”为祸网络，他们打造价值百亿的木马病毒产业链疯狂敛财……

翻开这一章，你将认识真正的黑客，纵观半个世纪黑客发展的足迹，了解黑客与程序之间的不解之缘，并洞悉黑客走过的捷径。

1.1 认识真正的黑客

从最初的青涩变得老辣，从最初的纯真变得复杂。他们既开发了首款计算机游戏，开拓出让人们欢乐忘忧的游戏世界，也编写了让无数用户陷入噩梦的木马程序和令人谈之色变的计算机病毒。他们是谁？他们就是伴随着计算机、网络发展而成长的特殊族群——黑客。

1.1.1 黑客发展简介

20世纪50年代的麻省理工学院（Massachusetts Institute of Technology，MIT）率先引入了分时系统，以使学生和教师可以接触最新的科技成果——大型计算机。在分时系统中，大型主机连接多套终端，主机CPU将时间划分成若干个称为时间片的片段，轮流为各个终端服务。理论上每个使用终端的用户，都能获得较满意的响应时间，几乎感觉不出与别人在共用计算机。然而，这只是理论而已，学生们获得的永远是最低等级的授权，只要教师或教授们登录，那学生就只能苦等了。

于是想平等使用大型主机的学生，便开始寻找系统的安全漏洞，修改优先权记录。这一类行为受到大量学生的追捧，为此他们还创造了一个新名词——Hacker（黑客），以褒扬那些手法巧妙、技术高明的计算机高手。Hacker这个听起来很“酷”的词，很快在学生中流传，并在数年之后形成早期的黑客文化——自由、分享。

20世纪60年代是第一代黑客发展的黄金十年。那时的黑客很纯真、很激情，他们还没有想到木马、病毒这些东西，只是想尽可能地扩展计算机的应用，将困在高科技计算、人工智能实验室和武器研究实验室中的计算机“解放”出来，以为更多的人服务。例如，在MIT人工智能实验室里（如图1-1所示）为实现计算机陪人玩游的设想而“挪用”实验室设备的史蒂夫•斯拉格•拉塞尔（Steve Russell）、格拉兹（S. Graetz）和考托克（A. Kotok）3名同学没少被导师训话。不过，当时估计谁也没想到，自此揭开了产值超百亿美元的计算机游戏产业，如图1-2所示。又如贝尔实验室的邓尼斯•里奇（D. Ritchie）和肯•汤姆森（K. Thompson），他们也同样“挪用”小型计算机，开发出UNIX操作系统，并说服AT &.T公司将此成果以低廉价格，甚至免费许可给学术机构及教学使用。

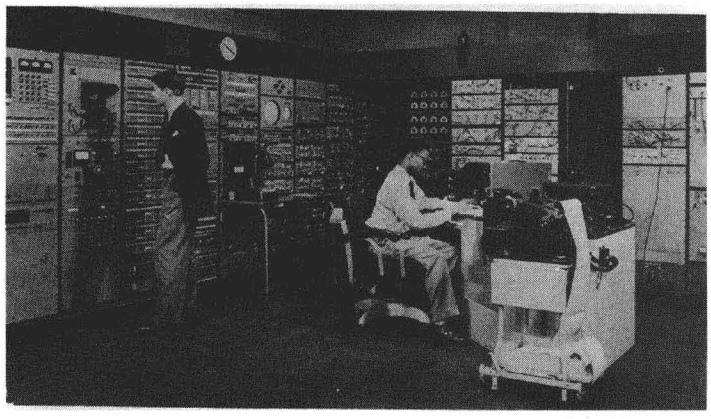


图 1-1　黑客最早的起源地——20 世纪 50 年代麻省理工学院人工智能实验室

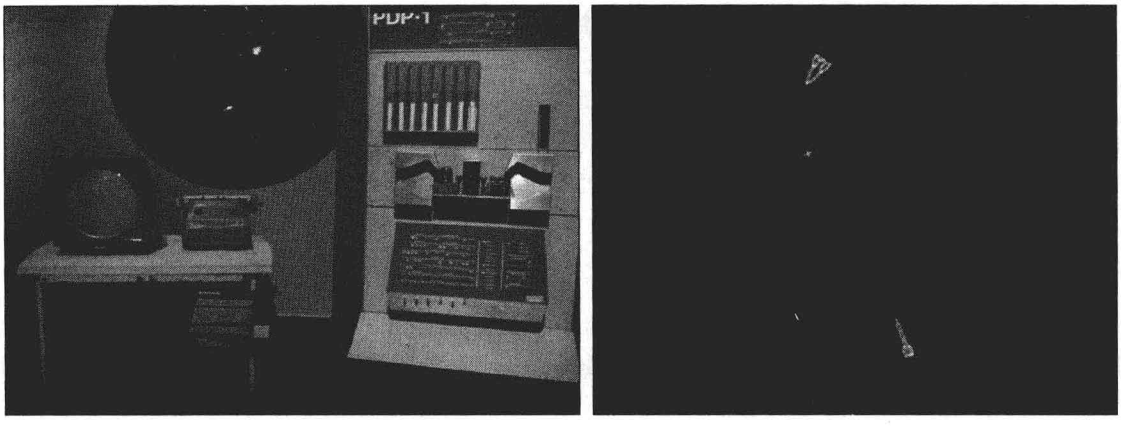


图 1-2　在人工智能实验室开发出的第一个电脑游戏——Spacewar

可以说，最早期的黑客对抗着整个信息不对称的旧工业时代，没有他们，精密的计算机可能依然被困于各种狭小的实验室中，成为科学家们的专宠。

20 世纪 70～80 年代，ARPANET 军用网络研发并开放部分功能给教育及科研机构使用。网络带来了黑客发展的另一个春天。通过网络，黑客将自由使用计算机、信息免费的观点发挥得淋漓尽致。对于这期间的故事，1985 年，美国《连线》杂志的记者 Steven Levy，采访了包含微软创造者比尔·盖茨、苹果电脑创造者沃兹和乔布斯（Steve Wozniak，Steve Jobs）等曾经的众多黑客，编写于 *HACKERS：Heroes of the Computer Revolution*（黑客：计算机革命的英雄）一书之中。这本书时隔 25 年后依然畅销不衰，如图 1-3 所示。其中在 True Hacker（真正的黑客）部分中介绍了 20 世纪 70 年代，MIT 的人工智能实验室、斯坦福大学人工智能实验室（SAIL）和卡内基梅隆大学（CMU）3 大根系黑客的起源及成长；在第 2 部分 Hardware Hacker（硬件黑客）中讲述了黑客们走出校园，在硅谷推动 PC 发展的过程；在第 3 部分 Game Hacker（游戏黑客）中介绍了商业文化与传统黑客精神的碰撞，以及黑客们如何在世俗金钱面前缴械投降。

随着时代的发展，计算机与网络已经演变成商务经济、交往沟通、游戏娱乐和政治宣传等的新舞台，已经不再是黑客们单纯研究技术的空间，传统的黑客也随着计算机领域环境的巨变而走进历史，但是黑客群体并没有消亡，新生代的黑客以更为多元化的价值观出现在我们眼前。

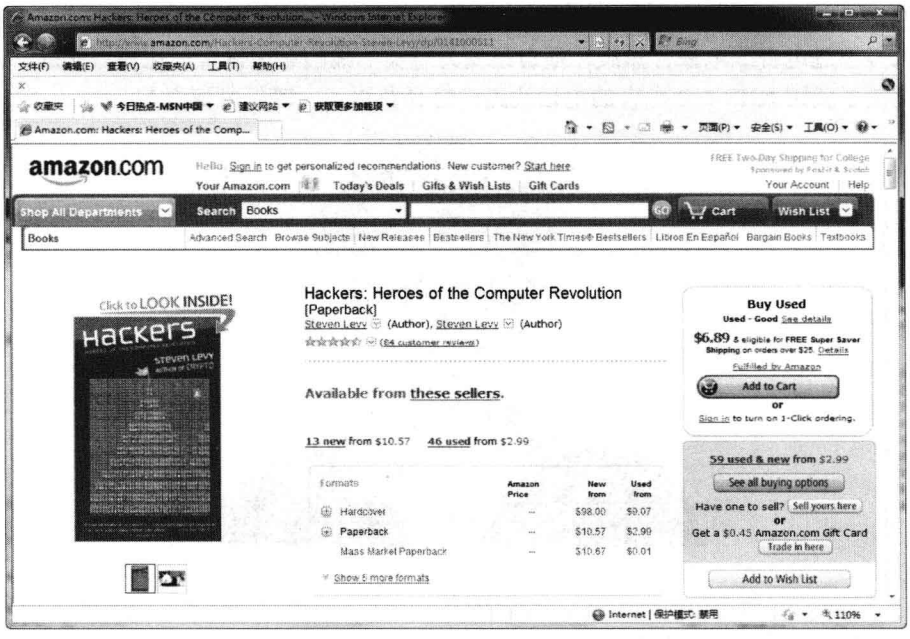


图 1-3　25 年畅销不衰，2010 年再版的 *HACKERS: Heroes of the Computer Revolution*

- 破解猎奇。凯文 • 米特尼克（Kevin David Mitnick，如图 1-4 所示）在他 15 岁时出于好奇破解并闯进“北美空中防护指挥系统”查看了当时的核弹部署，令美国当局为之震惊。事后，他还入侵了 FBI，将负责调查他的特工档案篡改为恶贯满盈的通缉犯。胡作非为的结果是，他在 16 岁那年，有幸成为世界上首位被关进少管所的黑客。
- 自由分享。AT &.T 收回了学术教育机构免费使用 UNIX 操作系统的授权，许多教育机构不得不改用其他操作系统，如 Minix 等其他廉价而简单的操作系统辅助教学。李纳斯 •托沃兹（Linus Torvalds，如图 1-5 所示对此十分不满，他编写了一套完全免费的开放系统——Linux，与收费操作系统较劲。

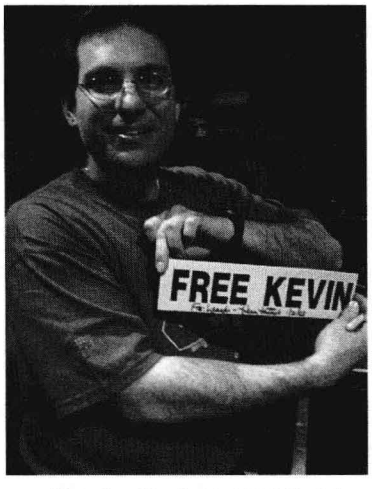


图 1-4　Kevin David Mitnick

图 1-5　Linus Torvalds

- 金钱至上。凯文•鲍尔森（Kevin Poulsen），绰号“黑色幽灵”，如图 1-6 所示，善于入侵并控

制电话线路。利用这一特长，他打听到哪里开展有奖热线活动，就掌握当地的电话线路，让别人打不进电台或电视台热线，把自己变为有奖热线的领奖常客。比较夸张的一次行动是，他控制了美国 KIIS-FM 电台的电话线路，轻易获得了一辆保时捷汽车。

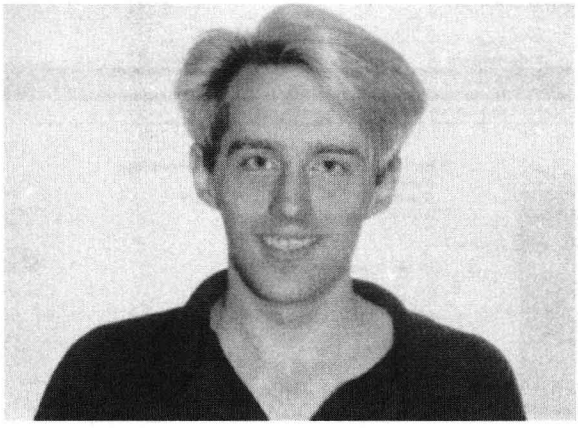


图 1-6　Kevin Poulsen

1.1.2　白帽黑客与黑帽黑客

尽管新时代黑客的行为及价值观日趋复杂，但是人们还是习惯性地将黑客分为两大族群——白帽黑客（white hat hacker）与黑帽黑客（black hat hacker）。

白帽黑客是指合法使用黑客技术的黑客，他们通常是学术研究人员或计算机安全顾问，在合法的情况下攻击指定的系统，以进行安全测试，寻找可能存在的安全漏洞，并协助用户解决各种安全问题。

IOActive 公司渗透测试总监 Dan Kaminsky 就是一位著名的白帽黑客，他在 2008 年发现了可能引发因特网大面积崩溃的 DNS 协议漏洞，协助 DNS 服务器管理员修复这个漏洞并及时发布了相关的补丁，以供更多有需要的管理员使用。又如 iSec Partners 公司的高级安全顾问 Zane Lackey，他专门发掘 Voip 通信中的问题，并协助相关通信公司解决这些问题，以为用户提供更优质的因特网音频通信。

黑帽黑客是指非法使用黑客技术的黑客，部分人也称他们为破解者（Cracker）。他们在法律许可范围外攻击家用计算机、商用服务器，以及政府网站，从而获得他们感兴趣的资料数据，控制对方的计算机。除此之外，相当多的黑帽黑客还大肆破解商务软件和机密档案以牟取暴利。

从两大阵营的描述不难看出，黑客技术实际上是一把双刃剑，既可以推动计算机应用，使网络服务更好地发展，也可以用于入侵和破坏。到底加入哪一阵营，只存乎技术使用者的一念之间。

1.1.3　他们是怎样成为黑客的

“如何成为黑客的？”每一个对黑客感兴趣的人都想知道这个问题的答案。对此，我只能告诉你：真正的、守法的黑客是崇尚自由、勇于挑战困难的群体。国外著名黑客作家 Eric S. Raymond，曾在 *How To Become A Hacker*（怎样成为一名黑客）一文中，给心存迷茫的入门者一首小诗：

To follow the path: