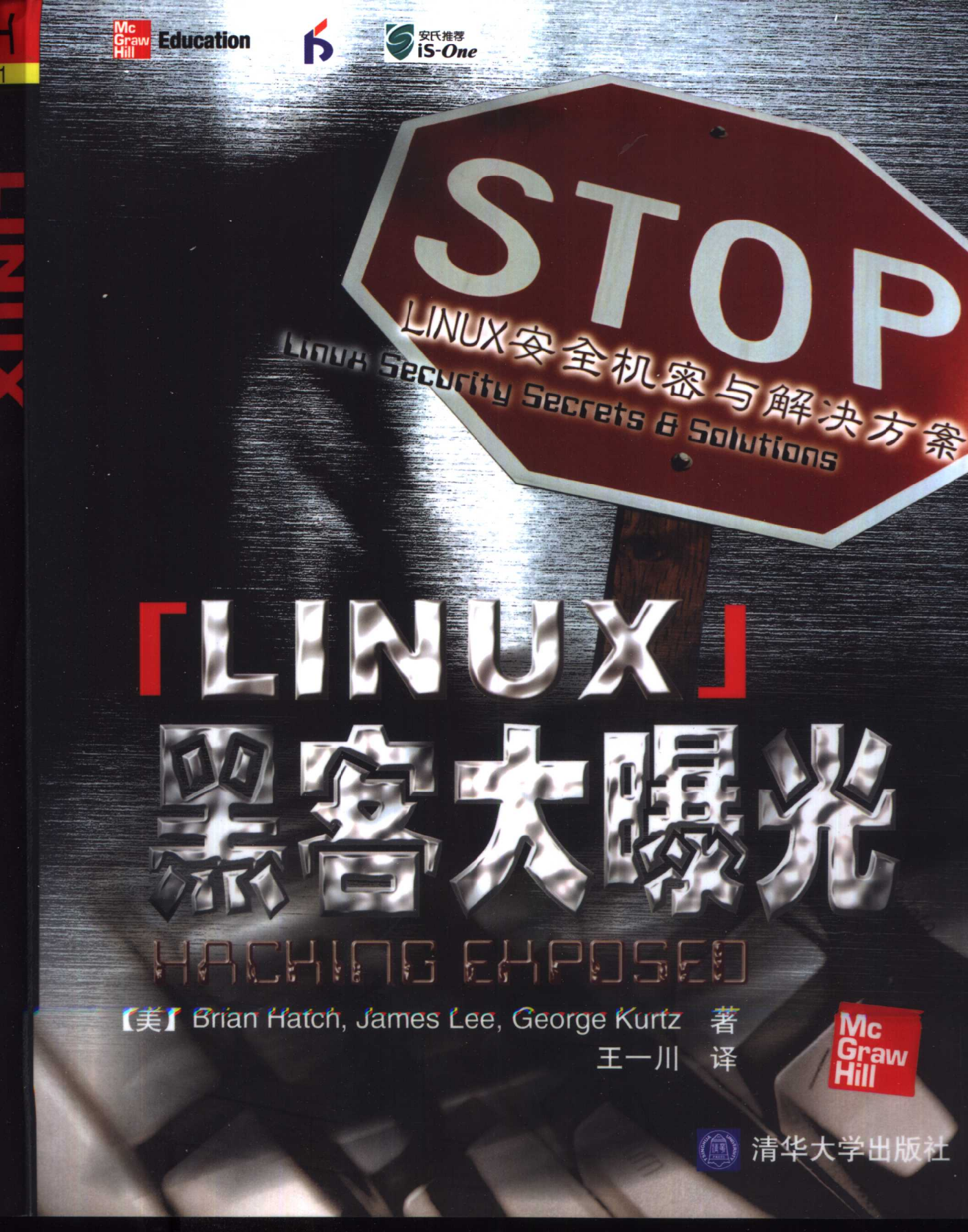
Mc Graw Hill Education
安氏推荐 iS-One
STOP
LINUX安全机密与解决方案
Linux Security Secrets & Solutions
「LINUX」
黑客大曝光
HACKING EXPOSED
【美】Brian Hatch, James Lee, George Kurtz 著
王一川 译
Mc Graw Hill
清华大学出版社

Linux 黑客大曝光

Linux安全机密与解决方案

【美】 Brian Hatch, James Lee
George Kurtz 著
王一川 译

清华大学出版社

（京）新登字158号

北京市版权局著作权合同登记号：01-2001-3277

EISBN 0-07-212773-2

内容提要

本书是《黑客大曝光》畅销书系列之一，主要针对Linux操作系统，从攻击者和防御者的不同角度系统阐述了Linux网络的入侵手段及相应防御措施。

全书以step-by-step的方式详细讨论了黑客的攻击方法，其中包括黑客收集信息、确定目标、提升权限、获得控制、架设后门和掩盖踪迹的方法；并述及各个Linux发布版本的安全特点及其细节，包括RedHat Linux，SuSE，Debian和Slackware。全书注重案例分析，讲解了很多具体攻击的过程，更重要的是对几乎所有讨论过的攻击手段都提供了相应的对策。

本书是安全漏洞的宝典，是负责Linux安全保障工作的网络管理员和系统管理员的必读之书，也可作为信息管理员以及对计算机和网络安全感兴趣的人员的重要参考书。

书　名：Linux黑客大曝光：Linux安全机密与解决方案
作　者：Brian Hatch，James Lee，George Kurtz
译　者：王一川
出版者：清华大学出版社（北京清华大学学研大厦，邮编100084）
印刷者：北京耀华印刷有限公司
发行者：新华书店总店北京发行所
开　本：异16　　印张：36　　字数：661千字
版　次：2002年10月第1版　　2002年10月第1次印刷
印　数：0001~6000
书　号：ISBN 7-302-05876-8/TP·3483
定　价：59.00元

序

当前的计算机和网络世界充满了与安全相关的威胁。尽管对统计数字有所怀疑不失为明智之举，但仍有可信的证据表明全球有超过3亿人在使用Internet。即便绝大多数用户在访问Internet时小心谨慎，但总有一小部分人不是这样的。不幸的是，这一小部分人已经产生了巨大的与其人数不成比例的影响。正是这些人打开了潘多拉魔盒，他们侵犯秘密、中断或拒绝服务、篡改数据和系统，甚至敲诈勒索和愚弄人。最不幸的是，这些人破坏了众多用户在正常参与中所得到的乐趣和信心。

几十年来，人们一直在尝试保护系统和网络的安全。我们见到过众多的关于安全的规范模型，以及大量声称能改进安全的工具。其间通过了新的法律，形成了众多的安全和执法团体。尽管与安全相关的会议、课程和认证在不断发展，但关于违反安全性的报告数量仍然急速增长。因此，必然有一些措施没有起作用。

本书代表了一种新的而且在不断更新的方法，本书是为数不多的详细阐述入侵者攻击Linux系统时真实行为的书籍之一。作者的意图是帮助读者真正了解存在的威胁——“眼见为实，耳听为虚”。一旦读者了解到这种威胁，就很容易领会到相应对策的必要性，以及激发对这些对策的工作机制的兴趣。这不是一本示意性的书籍，其中给出的对策与攻击手段一样切实可行。

自几年前Linux兴起以来，整个Linux社区急切盼望着与本书类似的书籍问世。用“星火燎原”来形容Linux群体的发展绝不言过其实。Linux极其类似于Unix，这既是福源也是祸因。福源意指学习使用Linux会更加容易。但是Linux社区太过经常地忽视安全问题，可能是因为人们以为Linux必然和Unix同样安全，后者近十年来在安全性方面有非常大的进步。未受保护的Linux系统现在已经被认为是整个网络世界中破坏和危险的最大潜在来源之一。本书旨在有效地“唤醒”那些对Linux安全性盲目自满的人，然后给这些感到震惊的沉睡者指明正确的方向。

E.Eugene Schultz, Ph.D., CISSP
加州大学伯克利分校实验室

安 氏 推 荐

Linux操作系统以令人惊叹的速度发展，如今Linux已经普遍应用于大型计算、企业应用服务、桌面应用等领域，可以说，Linux 已经进入我们的生活。

开源创造了今天的Linux，开源带给Linux无尽的力量，开源也使更多的漏洞显现在我们面前，同时开源也为我们提供了更多实现安全的方法。

这是一本《黑客大曝光》的Linux 专题的姊妹篇，如果您对于 Linux 安全持认真的态度，请您务必拥有这两本书。

像《黑客大曝光》一样，本书对关于Linux系统的每种攻击方法进行“曝光”、并有相应的攻击实例和对策。附录中还有一个完整的攻击过程。

当然，本书有些地方在内容上还不是很丰富，读者可以参考书中提供的网络链接和其他书籍。

当您正在或者准备应用Linux提供企业服务时，或者您想深入了解Linux的安全问题，不妨将这本书摆在案头，它会成为您通往Linux 安全之路的披荆斩棘的利刃。

关 于 作 者

Brian Hatch，照片中右边的那位，Onsight公司（http://www.onsight.com）的首席黑客，他是一位Unix/Linux和网络安全顾问。他的客户遍及各主要银行、制药公司、教育机构，以及加利福尼亚主要的Web浏览器开发商和幸存的网络公司。Hatch先生通过Onsight向各个企业讲授安全、Unix和程序设计方面的许多课程，他同时也是西北大学的助理讲师。在购入Apple Ⅱ作为他的第一个Unix系统之前，Hatch已保护和侵入过众多的系统。他也是Stunnel的共同维护者，这是一个开源的SSL安全软件包，广泛用于加密文本协议。

读者可以通过电子邮件brian@hackingLinuxexposed.com与Hatch先生联系。

James Lee，照片中左边的那位，是Onsight公司的CEO，该公司致力于开源软件技术方面的培训和咨询。Lee在软件开发、培训、Linux安全和Web编程方面有13年的经验。作为开源软件的提倡者，由于Linux的开放性和自由，他坚信Linux是稳定、安全和有趣的。他可以滔滔不绝地谈论Linux，Perl，Apache和其他开源软件产品的优点——这一点，可以问他的学生。他曾为*The Linux Journal*撰写过多篇关于网络编程和Perl的文章。

读者可以通过电子邮件james@hackingLinuxexposed.com与Lee先生联系。

George Kurtz是Foundstone公司（http://www.foundstone.com）的CEO，该公司是一个非常前沿的安全咨询与培训组织。Kurtz先生是国际知名的安全专家，在他的安全顾问生涯中已进行了数以百计的与防火墙、网络及电子商务相关的安全评估。Kurtz先生在入侵检测、防火墙技术、危机处理过程以及远程访问方案等方面有丰富的经验。他还在许多安全会议上发表演讲，其言论在很多杂志中被引用，包括 *The Wall Street Journal*, *InfoWorld*, *USA Today*和 *the Associated Press*等。Kurtz先生还经常被邀请在安全事件中发表评论，也是各大电视台（包括CNN，CNBC，NBC及ABC等）的常客。

读者可通过电子邮件george@hackingexposed.com与Kurtz先生联系。

前　言

20万读者的共识

《黑客大曝光》是由Stuart McClure、Joel Scambray和George Kurtz编写的畅销书，这本书赢得了巨大的尊重和高度的评价。黑客大曝光列举了在多个操作系统和网络设备中进行攻击的方法，在此之前没有一本书能达到它这样的高度。在有限的空间内涵盖这些系统也导致了一个问题，即读者不能够如其所愿地深入到足够程度。因此，我们创作了黑客大曝光系列的第2本书，即本书。

本书更为详细地阐述了Linux上的黑客行为，向大家展示了Linux与其他类Unix系统的不同之处，并给出了特定于Linux系统，同时也能立即实施的黑客对策。与《黑客大曝光》的重击风格一致，本书也专注于攻击方所使用的实际攻击手段。这些信息应该在有责任心的读者中共享，因为有那些不怀好意的人早已了解了这些技术，事实也确实如此。请读者们不要试图使用这些技术去侵入别人的Linux系统。本书使Linux黑客走下神坛，也使攻击者试图获得系统root权限的各种诡计大白于天下。

保护Linux系统的安全，已是其时

1991年，Linus Torvald还是Helsinki大学的一名学生，他有点像一名自学成才的黑客。那时，这个年轻的芬兰人爱好扩展计算机系统，但是没有一个系统符合他的需要，于是，Linux就诞生了。Linus是一个真正的黑客，他使用自己的技能引发了一场软件革命，其后有一批狂热的追随者。

不幸的是，现在“黑客”这个术语的含义已经发生了质的变化，从早年象征着世界上类似于Linus的天才程序员，到现在指平均13岁、能够自己下载别人的黑客代码并运行之，而且不受惩罚的那些人。与自1991年以来对安全问题的疏忽形成鲜明对比的，是这新一代的“恶意黑客”对于众多的系统尤其是Linux系统的攻击，这个问题部分源于Linux系统的广泛存在。

N

自从将内核代码张贴到USENET以来，Linux已经走过了很长的路，它不再是当初的业余系统。它的用户遍及全球众多大学以及财富500强企业。数以百万计的人们每天依赖于基于Linux的数据库、电子商务和关键系统。因此，一本完整的、致力于保护Linux安全的手册应运而生。

本书涵盖了恶意黑客攻击Linux系统的众多方法，以及这些方法的基本原理。针对那些攻击者精通于这些技术的情况，本书旨在以培养系统管理员的方式培养家庭用户。这些系统管理员不仅负责关键任务的Linux服务器的日常操作和安全保护，而且还得为生计而努力（他们的所得远低于他们的付出）。如果此书在你手边，说明你已经意识到安全的重要性。那么，不要放下这本书，继续学习这些网络攻击者用来攻击你的Linux系统的工具和技术，以及那些能够保障系统安全性对策。

Linux给用户带来了强大的功能和优越性。迄今为止，Linux的演化仍是一个传奇。客观而言，小系统能够做到这一点。现在，随着Linux演变成为一个非常稳定的操作系统，其复杂性使得在安全方面犯错误的机会也大为增加。

具备《黑客大曝光》的全部要素

本书建立在使得《黑客大曝光》成功的要素之上。我们将沿着黑客入侵系统的每一个步骤走完整个过程：

- ▼ 目标确定
- ■ 进入系统
- ■ 提升权限
- ▲ 掩盖踪迹

本书具备模块化结构，因此可以分成几个部分阅读。每一种攻击方法和对策都相对独立，读者可以根据自身情况安排阅读这些内容，并以本书讨论的方法修复出现的问题。

许多攻击都可以被同一种对策所抵御。为了避免重复阐述这些方法和方便读者查找同一方法的描述，我们将许多这样的通用方法分离出来，并将之放置到本书的开头，因此读者可以尽早掌握它们，以便在后续章节看到这些名词时理解它们的含义。同时，某些主题在本书中也拥有各自的章节，以突出其重要性。

为了便于阅读，图标与《黑客大曝光》（第2版）一致

本书都使用与下面类似的特殊图标来突出每一种攻击技术：

这是一个攻击图标

便于识别特定的穿透测试工具和方法。

每一种攻击都有某些实用的、并经过测试的相应对策，这些对策使用特定的图标：

这是一个对策图标

如果必要，就使用它来修复所揭示的问题。

本书还大量使用提高视觉效果的图标，强调经常被忽略的细节。例如：

相关站点www.hackingLinuxexposed.com是本书的重要部分，我们建议读者经常访问这个站点以获得更新信息、作者的心得，以及本书所提及的所有工具的链接和本书所包含的所有源代码，这样读者就不需要自行输入了。

本书对实例中的源代码、屏幕提示和图示做了清理，并对用户的输入以黑体字标出：

```
prompt# find/home/[p-z]* -name\*.tgz -print
/home/pictures/calvin.tgz
/home/pictures/lydia.tgz
/home/sprog/shogo.tgz
```

根据作者的共同经验，对于每一种攻击方法，都给出了基于三个组成部分的风险率：

流行度	*在实际的攻击中被使用的频率。1表示极少，10表示广泛使用。*
容易度	*执行攻击所需要的技巧等级。1表示不需技巧或极少技巧，10表示有丰富安全性经验的程序员。*
影响力	*在攻击成功后导致的潜在损害。1表示只泄露目标的无关紧要的信息，10表示超级用户帐户或类似的信息。*
风险率	*上述三个值的平均值四舍五入之后得到综合的风险率。*

关于机器名称和IP地址的说明

对于在例子中用到IP地址的情形，我们决定使用192.168.x.y，10.x.y.z或172.[16-32].x.y等类型的地址。这些地址在Internet上是禁用的（根据RFC-1918），只能用于本地内部网。也就是说，本书中的IP地址在Internet上是不能访问的，在本书中使用这些IP地址就如同在美国影片中使用555开头的电话号码一样。有时书中也使用一些显然就是不合规定的地址，如123.267.78.9。在这里，267明显是假的，因为IP地址中每个字节的合法值在0~255之间。

警告 *RFC-1918中禁用的IP地址可能在读者的内部网上出现，因此我们建议您不要以所给的IP地址使用那些例子，以免出现自己攻击自己的情形。*

例子中用到的那些域名也是不合法的。例如machine1.example.org（example.{com|net|org|edu}类型的域名是专门用作举例的——没有一台主机会使用.example.xxx的域名）就是一个虚拟域名。同时，我们也在域名中使用下划线，例如www.illegal_name.net。在域名中，下划线是不合法的。

本书这样做的原因很简单：不对Internet上任何一台特定的机器予以额外关注。很多情形下，人们把潜在可利用的代码张贴到Internet，同时认为读者会将代码中的机器名替换成实际的目标机器名。然而，也有很多人（主要是那些脚本小子）只会依原样运行这些代码，从而导致无辜站点被攻击。通过将域名和IP地址都设为非法值，我们希望能够使人们摆脱这种困扰。

本书的组织结构

第1部分　锁定Linux目标

Linux日益流行。那些只使用过黑盒操作系统的人们，在腾出硬盘空间并第一次安装Linux之后，就会发现开源运动的乐趣所在。

第1章　以对Linux的简要概述开始，接着介绍内建于Linux操作系统的安全措施。经验丰富的Linux系统管理员会发现其中的大部分内容都已经耳熟能详了。这些内容所针对的是那些Linux系统管理员新手，以使他们尽快入行。本章也涉及了Linux和其他类Unix系统的差异，并讨论了仅在真正的多用户操作系统上才出现的问题。

第2章 整章详述各种黑客对策。在本书随后的章节中都将引用到这些手段和策略。本章的目的在于使读者尽早熟悉它们，以便在讨论攻击方法时，能随时想到这些对策。这样，当读者随后看到书中所涉及的攻击手段时，甚至能够预言可使用哪些对策。

第3章 进入正题：攻击者如何发现并检查你的系统。读者将会了解到攻击者如何在Internet上数以百万计的计算机中选中你的机器，确定你所运行的系统，并在试图侵入之前进行研究。

第2部分 由外入内

在攻击者搞乱你的系统之前，他必须先从外部进入你的系统。有很多种方法可以进入你的系统。

第4章 首先给出黑客直接或间接使用的某些诡计。这里讨论社交工程(social engineering)，即黑客取信于人们并使之放松警惕的过程。我们将向读者展示黑客如何通过欺骗，使人们运行他所提供的工具，从而如其所愿危及受害者的系统安全。

第5章 黑客也可以直接从控制台破坏系统。不论如何保护系统使之免受来自网络的攻击，对计算机有物理访问权的黑客仍可以使用很多方法，包括从通过软盘启动他自己的操作系统，到从机器里拔出你的硬盘等。

第6章 当前大多数对系统的攻击来自于网络上的黑客。本章包括多种直接针对系统以获得非授权访问的攻击方法，例如对网络守护进程的缓冲区溢出和输入验证攻击，轰炸拨入以查找未受保护的调制解调器，在网络上运行口令猜测程序，以及嗅探网络连接以获取有用的数据等。

第7章 介绍一些基于恶意使用网络和网络协议的黑客手段。包括DNS高速缓存破坏(DNS cache poisoning)、篡改网络路由、滥用IP相关信任、中间人攻击以及可怕的拒绝服务攻击(已经折磨过多个著名站点)。这些攻击手段的目的并不是获取系统权限，而是会对站点所提供的服务、数据以及可靠性产生巨大影响。

第3部分 本地用户攻击

如果黑客具有系统的本地用户权限，其攻击手段要远多于源于外部的攻击。一旦登录到系统，黑客通常会试图巩固其桥头堡。

第8章 黑客找到登录系统的方法并不意味着他可以马上获得超级用户权限。但是，一旦他获得用户帐号，就能够看到系统中存在的可经由网络利用的其他不安全因素。攻击者期望能突破root帐号，以作为他的战利品，那样整个系统就在他的掌控之下了。

第9章 口令是访问计算机的关键。通过攻击，黑客可以获取系统中的加密口令，并试图破解它。这些口令可以用作攻击新的系统的踏脚石（因为很多人在多台机器上使用同样的口令），也可以帮助他们在被发现和系统重启之后再次进入系统。这其中也可能包括root口令。本章将深入讨论黑客用来攻击系统和预防这些攻击的几种工具。

第10章 给出了黑客在侵入之后用来保护其自身的几种方法。包括编辑日志文件以掩盖踪迹，创建后门以便将来进入，设置特洛伊木马以隐藏实际行为，甚至修改内核本身以防止被发现等。

第4部分 服务器安全问题

Internet服务对Linux机器的依赖性日益增加。这些服务对于个人和商业公司同样重要，因此我们认为有必要在本书中深入介绍一些最常见的服务。

第11章 讨论安全问题的历史以及邮件服务器Sendmail，Postfix和Qmail的常见配置问题。这3个软件组成了Internet上几乎所有类Unix主机上的邮件服务器。

本章也讨论了FTP服务器、客户端和FTP协议本身的问题。尽管使用HTTP进行文件下载日益流行，但FTP仍然广泛使用，因为它同时支持下载和上传。近些年来，绝大多数FTP服务器都曾遭遇过大量的安全问题。本章将讨论更好地保护FTP服务器的方法，以及既可满足需要又能减少安全风险的其他替代方案。

第12章 Internet的繁荣在很大程度上源于HTTP和Web服务器的出现。似乎世界上的每个人都拥有自己的主页或域名，很少有公司没有主页，至少已有创建主页的计划。同时多数主页所提供的不仅仅是静态页面，动态页面已经成为Web上进行用户交互的主流。

当前多数常见的安全问题起因于Web服务器的错误配置，或者为了支持用户交互而使用了不安全的程序。错误丛生的CGI程序在Internet上到处可见，而且实际上也被某些Web服务器四处扩散。关闭Web服务器显然不是一个解决办法，因此本章讨论了多种程序缺陷和配置问题，以便读者在提供主页服务时加以注意。

第13章 介绍几个向Internet开放特定服务的方法。讨论基于TCP包的用户层访问以及基于ipchains和iptables的核心层控制。通过限制可以连接到网络服务的机器，可以大幅减少服务器受到Internet攻击的机会。

第5部分 附录

在附录中，给出了简单的step-by-step指令，以帮助读者保护系统安全。

附录A 给出了升级系统安装软件的详细方法，针对Red Hat，Debian和Slackware等不同操作系统的软件包管理器分别给出了相应的信息。

附录B 给出了关闭服务的方法，从而减少攻击者可以利用的途径。首先讨论了启动进程init，然后针对Red Hat和SuSE分别给出了相应的命令集。

附录C 在网上有许多在线资源，通过访问它们，可以充分了解当前热点问题及你的系统的脆弱性。我们列出了一些最重要的URL，包括开发商和安全性问题的邮件列表、安全和与黑客方法相关的站点和新闻组，以使读者在所关心的安全问题上保持耳目灵敏。

附录D 本书涵盖了导致不同程度损害的各种攻击方法。在现实世界中结合使用这些方法很重要，因此在这个附录中，我们从始到终，逐命令逐步骤地介绍在Internet中曾经出现过的几个实际攻击。这种扩充型实例使用到的方法遍及本书，诸多细节将有助于读者融会贯通本书的安全概念。

致读者

我们通过长时间的辛勤工作，编著了这本与《黑客大曝光》的书名相对应的有关Linux安全的书籍。在度过了众多的不眠之夜，本书终于付印，我们希望读者将会发现本书以及相应的站点是保护系统安全的有力工具。

借用古人的一句话，“胜利属于犯了倒数第二个错误的参与者”。为了保护你的Linux系统安全，不要犯最后一个错误。请阅读本书。

目　录