Mc Graw Hill Education

“一本令人敬畏的参考书。尽管作者着重于Linux安全问题，但其中的许多条款、技术、工具和讨论贯穿了信息安全的各个方面。”

——ComputerWorld

Linux Security Secrets & Solutions

Hacking Linux Exposed , Second Edition

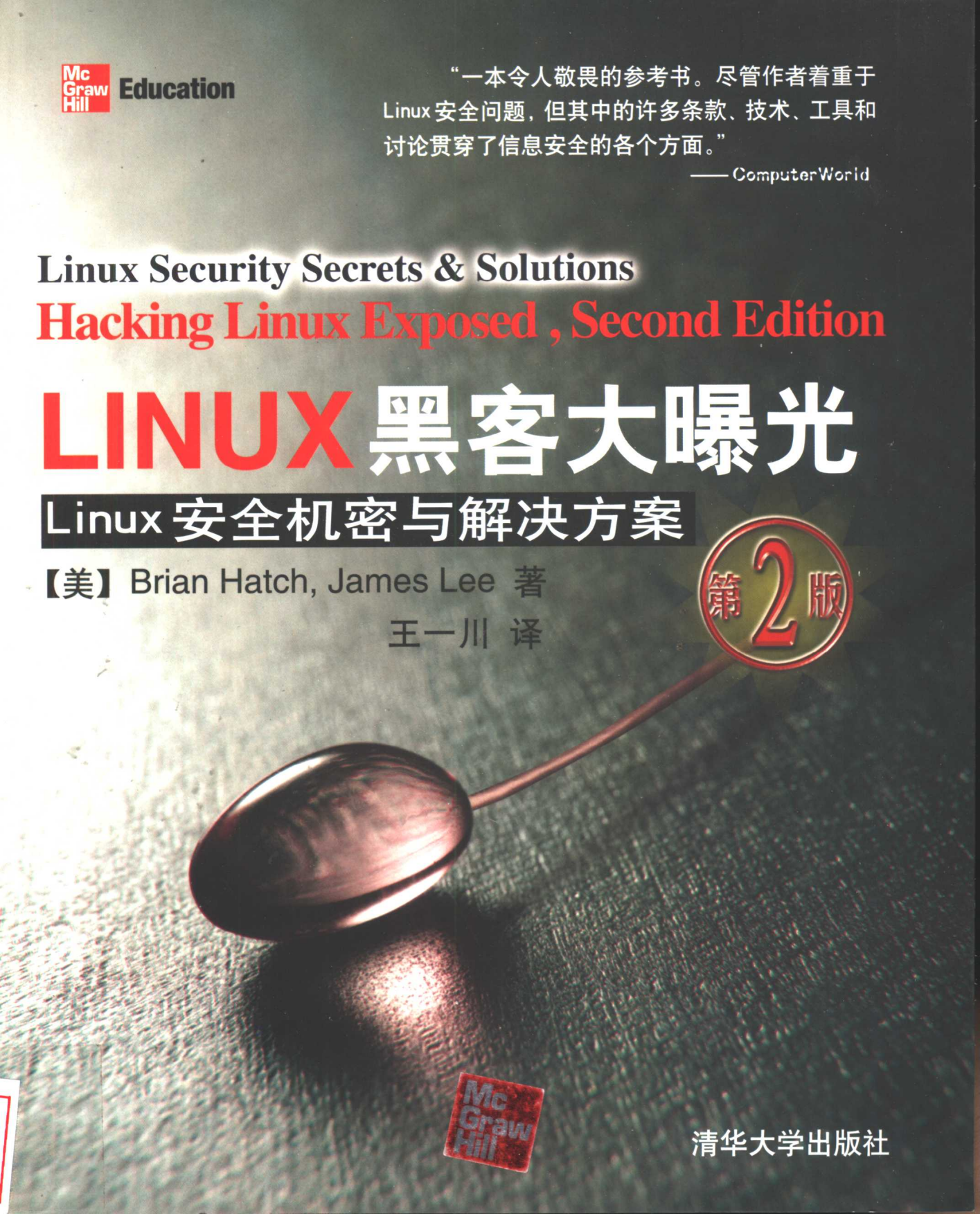
LINUX黑客大曝光

Linux安全机密与解决方案

第2版

【美】Brian Hatch, James Lee 著

王一川 译



清华大学出版社

Linux 黑客大曝光

Linux 安全机密与解决方案（第 2 版）

Hacking Linux Exposed

Linux Security Secrets & Solutions, Second Edition

【美】 Brian Hatch
James Lee 著
王一川 译

清华大学出版社
北京

Brian Hatch，James Lee
Hacking Linux Exposed，Second Edition
EISBN 0-07-222564-5

图书在版编目（CIP）数据

Linux 黑客大曝光：Linux 安全机密与解决方案（第 2 版）/
（美）哈茨（Hatch, B.），（美）李（Lee, J.）著；王一川译.
—北京：清华大学出版社，2003
书名原文：Hacking Linux Exposed，Second Edition
Linux Security Secrets & Solutions
ISBN 7-302-07655-3

I. L…　II. ① 哈… ② 李… ③ 王…　III. Linux 操作系统—安全技术
IV. TP316.89

中国版本图书馆 CIP 数据核字（2003）第 106645 号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**：100084
社 总 机：010-62770175　　**客户服务**：010-62776969

组稿编辑：科海
文稿编辑：陈洁
封面设计：曹映红
版式设计：卞雨桂
印 刷 者：北京市耀华印刷有限公司
发 行 者：新华书店总店北京发行所
开　　本：异 16　　**印张**：36　　**字数**：786 千字
版　　次：2003 年 12 月第 1 版　2003 年 12 月第 1 次印刷
书　　号：ISBN 7-302-07655-3/TP・5616
印　　数：1～4000
定　　价：59.00 元

Linux 黑客大曝光(第2版)

"以往经验表明，谁都不希望自己高度配置的系统被入侵。您可以选择自行摸索系统安全的艰难之路，或者选择购买这本书并学习其中的黑客技巧来保护自己。这本书为希望确切了解 Linux 系统所面临的安全威胁以及相应对策的人提供了这些来自多年实践的集体智慧的结晶。非常棒！"

——Dave Wreski，Guardian Digital的CEO，《Linux Security HOWTO》的合著者

"本书对Linux安全有深入的洞察力，为Linux系统的攻击和防御方法都提供了相当的细节。对于那些希望保护Linux系统安全的管理员而言，是一本必备书。"

——Huagang Xie，LIDS(Linux Intrusion Detection System)创建者

"《Linux黑客大曝光》（第2版）无愧于黑客大曝光系列的荣耀。不同层次的UNIX系统管理员都将得益于本书对系统漏洞细节的深入挖掘。本书组织清晰，逻辑性强，并穿插了作者搜寻到的各种有价值工具的介绍。"

——Fyodor，探测工具和安全扫描器Nmap的创建者

"作者完成了一项伟大的工作：以经典的黑客大曝光风格阐述Linux安全。本书覆盖了保障Linux系统安全性的所有层面：从安全基础直到底层细节。第1版的读者将对第2版所扩展和更新的部分感到满意。"

——Ryan Russell(Blue Boar)，Vulnerability Discussion邮件列表的创建者和早期管理者

"本书涵盖了从真实可靠的技巧直到锋锐的黑客手段之间的所有层面。如果您对Linux及其安全性持认真态度，请购买这本书。这就是我所要告诉你的。"

——Simple Nomad，Hack FAQ的作者

内 容 提 要

本书是原《Linux 黑客大曝光》的升级版，书中更为详细地阐述了 Linux 黑客不断演绎的行为以及应对策略。

全书分析现今最通晓战术应用的黑客的思路，以循序渐进的方式介绍如何预防最新的特定于 Linux 系统的攻击。书中详细介绍了攻击者如何收集信息、确定目标、搜寻漏洞和获得控制的方法，囊括了一些众所周知或迄今仍鲜为人知的入侵案例，通过对这些案例的分析，讲解了具体攻击的过程，以及提供这些攻击的详细对策。

本书是预防 Linux 安全漏洞的工具书，也是负责 Linux 安全保障工作的系统管理员必读之书，同时可供信息管理员以及对计算机和网络安全感兴趣的人员参考。

关于作者

Brian Hatch 是 Onsight 公司（http://www.onsight.com）的首席黑客，同时也是一位 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、Linux 和程序设计方面的许多课程，他同时也是美国西北大学的助理讲师。其黑客生涯开始于购入 Apple II+作为他的第一个 Unix 系统之前，迄今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，被广泛地用于加密明文协议。此外他还每周撰写“Linux Security:Tips,Tricks,and Hackery”时事通讯（位于 http://lists.onsight.com/），并且是《Linux 黑客大曝光》（第 1 版）的第一作者。读者可以通过 brian@hackinglinuxexposed.com 与 Hatch 先生联系。

James Lee 是 Onsight 公司（http://www.onsight.com）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 15 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。Lee 先生也是《Linux 黑客大曝光》（第 1 版）的合作者。读者可以通过 james@hackinglinuxexposed.com 与 Lee 先生联系。

关于丛书顾问

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 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，FOX 及 ABC 等）的常客。Kurtz 是畅销书《黑客大曝光》的所有三个版本的合作者。读者可以通过 george@hackinglinuxexposed.com 与 Kurtz 先生联系。

关于技术评阅者

Tom Lee 是 Foundstone 公司的 IT 经理。他是《Windows XP Security》的合作者，并且是《黑客大曝光》（第 3 版）和《黑客大挑战 2》的技术编辑。他有 10 年以上的系统管理和安全问题的工作经验。在加盟 Foundstone 之前，他就职于加利福尼亚大学 Riverside 分校。

前 言

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，因为那些不怀好意的人早已了解了这些技术，事实也确实如此。只有这样，现有的这些用以秘密侵入 Linux 系统的攻击技术才不会造成进一步的损害。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。

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到财富 500 强企业。数以百万计的人每天依赖于基于 Linux 的数据库、电子商务和关键系统；这样，一本完整的致力于保护 Linux 安全的手册的出现恰逢其时。

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。针对那些坏家伙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的对策。

第2版的新增内容

在编写本书第 2 版时，我们希望确保其独立性。第 2 版压缩、裁减并在某些情形下删除了一些旧的素材，从而为将近 200 页的新内容和 3 个新章腾出了位置。我们将第 1 版中的某些节移出并放置到本书相关的主页中，以在不牺牲质量的前提下为新增内容让路。第 2 版在内容编排上也做了某些重要的调整。一些更为常见的内容被移到相对靠前的位置，如缓冲区溢出和格式化字符串攻击。拒绝服务攻击单独列成完整的一章，此外，针对攻击者侵入系统后的行动增加了一个新的部分。第 2 版除了引入新的工具和攻击方法之外，对经典黑客工具的讨论当然也针对其新版本和新特性。

本书建立在那些使得《Linux 黑客大曝光》（第 1 版）成功的要素之上。我们将沿着黑客入侵系统的每一步骤走完整个过程：

- 目标确定
- 进入系统

- 提升权限
- 掩盖踪迹

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使读者折返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，以便在其后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，图标与第1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。

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：

注意　技巧　警告

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、屏幕提示和图示进行了清理，并以黑体字标出用户的输入：

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

本书在命令行提示符中指明当前用户。以#结尾的提示符表明当前必定是 root，而以$结尾的提示符表示当前是普通用户。提示符中可以包含用户名、机器名或路径信息等，例如：

jdoe$	用户 jdoe
server$	server 机器上的任何非 root 用户
root@crackerbox#	crackerbox 机器上的 root 用户
anurup:/etc$	用户 anurup,当前目录为/etc

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表示被广泛使用。*
简单度：	*执行攻击所需要的技巧等级，1表示有丰富安全性经验的程序员，10表示不需技巧或极少技巧。*
影响力：	*在攻击成功后可导致的潜在损害，1表示只泄露目标的无关紧要的信息，10表示超级用户账户或类似的信息。*
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。***

Linux Security:Tips,Tricks and Hackery

在本书的相关站点 http://www.hackinglinuxexposed.com/ 可以订阅由作者 Brian Hatch 执笔的时事通讯“Linux Security:Tips,Tricks and Hackery”，每周刊登与个人密切相关的 Linux 和 Unix 安全问题。与充满含糊其词的解答和夹杂着产品广告的传统专栏不同，“Linux Security：Tips，Tricks and Hackery”只登出可以直接应用的范例和源代码。其历史邮件归档于 http://www.hackinglinuxexposed.com/articles/。

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可怜人们，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都已经耳熟能详了；这些材料所针对的是那些 Linux 系统管理员新手，以使他们尽快入行。这里也涉及了 Linux 和其他类 Unix 系统的差异，并讨论了那些仅在真正的多用户操作系统上才出现的问题。此外还分类讨论了那些贯穿于本书的常见安全漏洞和概念。

第 2 章　整章详述各种黑客对策，例如日志文件分析。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，他必须从外部进入。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特洛伊木马，从而侵入相关系统。此外，还介绍了给人们日常工作带来烦恼的病毒和蠕虫。

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可以使用很多方法，包括通过软盘启动他自己的操作系统，直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，针对网络守护进程的缓冲区溢出和格式化漏洞攻击、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 和 ARP 高速缓存破坏、篡改网络路由、滥用 IP 相关信任、中间人攻击以及针对日益流行的无线局域网的攻击。

第3部分 本地用户攻击

如果黑客拥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，一旦他获得用户级账号，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 账号，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 使用强口令的安全认证并且使用可插入认证模块（PAM，Pluggable Authentication Modules）是计算机访问控制的关键。通过攻击，黑客可以获取系统中的加密口令，并试图破解它。这些口令可以用做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。此外也将介绍 PAM，它能够以灵活的方式为 Linux 应用程序添加强认证机制。

第4部分 服务器的安全问题

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而言同样重要，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 10 章 讨论安全问题的历史以及邮件服务器 Sendmail、Postfix、Qmail 和 Exim 的常见配置问题。这四个软件包组成了 Internet 上几乎所有类 Unix 主机上的邮件服务器。

第 11 章 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，FTP 仍然广泛使用，因为它同时支持下载和上传。这些年来，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。看起来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破坏问题起因于 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。错误从生的 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。首先，讨论基于 TCP 封装器、inetd 和 Xinetd 的访问控制方法。然后介绍了防火墙和如何使用 Netfilter(iptables)实施内核级访问控制。通过限制哪些机器可以连接到所提供的网络服务，可以大幅减少服务器受到 Internet 攻击的机会。

第 14 章 随着时间的推移，Internet 上放置了越来越多的 Linux 服务器，它们作为 IT 基础设施的重要性也日益增加。那些不能侵入目标系统的破坏者可能会转而谋求通过拒绝服务或分布式拒绝服务攻击将该系统从网络上断开。这类攻击并不总以获得系统的访问权限为目的，但能够对系统所提供的服务和数据的安全性及可靠性产生巨大影响。

第5部分 侵入之后

恶意黑客侵入系统之后，会采取步骤以防止入侵被发现，并确保自己将来对系统的访问权。

第 15 章 入侵者有很多种方法将自己隐藏在系统管理员的眼皮底下。他可以将本地的二进制系统程序替换为不显示其活动的版本，从隐藏目录运行其软件，以及删除可能指明其踪迹的日志记录。他还可以加密自己的通信连接，甚至使用防火墙，从而使入侵检测系统难以监视和发现他对系统的秘密访问。

第 16 章 入侵者将在系统中设置多个后门，以确保即便最初侵入点被清除之后也能够保留访问权。这包括正常的更改系统配置以允许他无口令访问甚至是 root 账号，或者植入特洛伊软件以便通过非常规方式获得系统访问权。

第 17 章 介绍入侵者隐藏踪迹和保持 root 权限的高级方法。首先介绍可加载内核模块（Loadable Kernel Module）和其他内核修改方法，从而使管理员即便使用干净的工具也不能发现系统的运行真相。随后，以对 rootkit 的介绍结束本章，这一工具能够快速地在系统中设置后门。

第6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 系统迟早会被侵入。这里介绍了侵入后恢复或重装系统并抵御再次入侵的方法。

附录 B 给出了升级系统所安装的软件的详细方法，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 C 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，然后针对不同的 Linux 发布分别给出了相应的命令集。

附录 D 本书涵盖了可能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，我们自始至终逐命令逐步骤地介绍在 Internet 中曾经出现过的实际攻击。这个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，编著了这本名副其实的安全著作的第 2 版。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 Chessmaster Savielly Grigorievitch Tartakower 的一句话，“胜利属于那个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

第1部分 锁定Linux目标

第2部分 由 外 入 内

第3部分 本地用户攻击

第4部分 服务器的安全问题