HZ BOOKS

Real World Linux Security:
Intrusion Prevention,
Detection, and Recovery

Linux与自由软件资源丛书

Linux安全

入侵防范、检测和恢复

附赠
CD-ROM

(美) Bob Toxen 著

前导工作室 译

机械工业出版社
China Machine Press

PH
PTR

Linux与自由软件资源丛书

Linux安全：入侵防范、检测和恢复

（美） Bob Toxen 著
前导工作室 译

机械工业出版社
China Machine Press

本书介绍Linux系统安全维护的技术。主要内容包括：一般性安全问题、高级安全问题、安全策略、信任机制以及猝发入侵和最近的入侵方法，如何为入侵做准备，如何进行入侵检测，如何成功、安全、快速地从遇到的入侵中进行恢复等。本书内容丰富、章节安排合理，适合广大Linux或UNIX系统管理员以及对安全方面感兴趣的读者阅读。附带光盘包括安全性监视工具软件。

本书版权登记号：图字：01-2001-0492

图书在版编目（CIP）数据

Linux安全：入侵防范、检测和恢复 /（美）托克森（Toxen, B.）著；前导工作室译. -北京：机械工业出版社，2001.11
（Linux与自由软件资源丛书）
书名原文：Real World Linux Security: Intrusion Prevention, Detection, and Recovery
ISBN 7-111-09383-6

Ⅰ.L… Ⅱ.①托…②前… Ⅲ.Linux操作系统-安全技术 Ⅳ.TP316.81

中国版本图书馆CIP数据核字（2001）第066773号

机械工业出版社（北京市西城区百万庄大街22号 邮政编码 100037）
责任编辑：谢 晨
北京昌平奔腾印刷厂印刷 · 新华书店北京发行所发行
2002年1月第1版第1次印刷
787mm × 1092mm 1/16 · 33.25印张
印数：0 001-5 000册
定价：67.00元（附光盘）

译者序

Linux操作系统是一种开放源代码的类UNIX操作系统，虽然它最初只是由一些爱好者通过互联网络协作开发出来的，但是经过几年的发展，已经有专门的公司负责它的内核测试以及应用工具的开发和测试。Linux是一种稳定的操作系统，安装和使用方便，功能强大，它几乎在任何硬件上都能快速运行且很少出现故障。它没有什么缺点，其广泛的使用保证了其缺点可以尽可能早地被发现并加以纠正。Linux具有多样性，它可以做得像UNIX系统一样安全。Linux已经被越来越多的个人甚至公司、企业和政府部门使用。勿庸讳言，它比不开放源代码并且漏洞百出的商业操作系统更得人心。

Linux的产生、发展和如今的流行无不得益于互联网络，特别是Internet。Linux本身对网络应用的支持也几乎是无可挑剔的，Linux和Internet就是这样形成了一种良性互动。在如今的Internet上，有许许多多的Linux系统提供了各种各样的网络服务。

任何一个多用户的操作系统都要处理系统安全方面的问题，连入Internet的系统面临更多的安全隐患，Linux也是如此。如今关于网站被黑客攻击的报告几乎每天都可以见到，而且随着网络应用的丰富多样，攻击的形式和方法也千变万化。

任何一个操作系统都不是完全安全的。如何增强Linux系统的安全性是Linux系统管理员最关心的问题之一，一个合格、敬业的系统管理员应该勇敢地面对并认真思索自己面临的任何安全问题。

我们紧跟国际计算机图书市场，急用户之所急，组织了几名有丰富的Linux使用经验和网络知识的专家翻译了这本《Linux安全：入侵防范、检测和恢复》，以飨读者。本书的作者有26年的UNIX/Linux使用经验，他是Berkeley UNIX的168个公认的开发者之一。本书的内容丰富准确、章节安排结构合理且由浅入深，实在是一本难得的Linux系统安全维护指南。并且本书中所讨论的安全方面的知识对于其他操作系统的管理和使用人员也有很好的作用。

本书由徐进辉、丁滟、王璐珍、苏湘玉和李春江组织翻译，前导工作室全体工作人员共同完成了本书的翻译、录排、校对等工作。全书最后由肖国尊统稿。由于时间仓促，可能存在个别翻译错误的地方，请读者批评指正。

2001年5月19日

序　言

现在在你手中的这本书，是我等了好几年才读到的，它是帮助你向Linux系统迈进的一个实用和方便的指南。同时，本书详尽论述了UNIX系统安全及计算机安全方面的大量知识。当我阅读这本书时，我已经把本书所涉及的所有规范都在我家里的Linux系统上测试过了。Bob Toxen的这本书既方便、简洁，又极富知识性，非常适合忙于工作的系统管理员从实际应用过渡到理论的学习。同时我还注意到，Bob对攻击路径、安全环及费用函数的介绍，给我们提供了一个简要的对安全性进行定量分析的统一框架。

负责安全工作的每个系统管理员都需要按照本书描述的步骤进行工作，但这只是应付今天的攻击的方法。为了防止明天的威胁，你还需要从整体的角度上来看待安全问题，而不仅仅是从某个攻击或攻击路径的层面上来看问题，应该从系统设计原则及总体方案的高度来看待安全问题，而本书最有价值之处也正是这一点。通过阅读本书，你将不仅学到日常的补救措施，还将可以学到一种在安全方面的风险与成本之间进行均衡的一种整体思考方法，未来受攻击的可能性，以及各层防护的功能及代价等。

像程序设计一样，安全是一门艺术。安全的最底层是机器，而一旦机器可以自动工作，你就可以开始考虑更好和更合适的基本安全技术以适应你的程序设计、特殊应用、安全等方面的需要。在安全的最高层，当机器和技术都趋于自动化后，专家的理论知识就会成为你非常有效的工具。在这两个层次中，你都可以根据本书所介绍的内容以及你自己的思考而总结出很多有用的东西。

Bob Toxen把安全的基本技术和专家的理论知识相结合，这是本书的特别之处。我想，你一定可以体会到其中的精彩之处，并由此而开始以全新的方法来思考你的Linux系统的安全。

Eric S.Raymond
2000年9月

目　录

第三部分 入侵检测

第四部分 入侵恢复

第五部分 附 录

第1章 导 言

Linux是一种稳定的操作系统，其安装和使用方便且功能强大，它几乎在任何硬件上都能快速运行，它很少出故障。Linux几乎没有什么缺点，由于它使用得非常广泛，所以其缺点能够及早被发现并改正。Linux是通用的操作系统，它可以达到和UNIX系统一样的安全性。

但是，每天都有Linux和UNIX系统受到入侵，原因不是它们本身不够安全，而是用户对将该系统安全地放到实际的世界——Internet——中的步骤不清楚。本书的目的就是教所有的Linux和UNIX系统管理员如何保护其系统，使其系统处于安全状态，使系统管理员确信已经采取了所需的安全措施。

1.1 本书适合的读者

本书将帮助Linux和UNIX系统管理员处理黑客入侵及用户误操作，以使其系统和网络尽可能安全。本书既介绍了弥补各种脆弱之处的又快又简单的解决方法，又介绍了一些非常复杂的解决方法。

本书的组织可以使繁忙的系统管理员一步一步提高系统的安全性，我们认为没有人可能在一周之内关闭系统而且专门研究其安全性。现实中，一个系统管理员的工作包含许多不能耽搁的任务，而且系统是如此重要，根本不能关闭这么久。

在现实世界中，尽管系统管理员付出了很多努力，但也不能完全抵挡住别人的入侵，本书用大量篇幅来介绍和处理可能的入侵，包括如何对入侵做准备，如何检测入侵，如何迅速完全地恢复系统以及如何保证数据和金钱的损失最小、波及面最小，为用户和老板提供最大的方便，这是本书的独特之处。

> 在2000年3月30日，来自世界各地的黑客在以色列召开会议，组织者宣称他们曾侵入以色列28%的计算机，这个百分数同样适用于整个世界。当然这是得到了计算机管理员允许后的尝试，上面的数字不会因为操作系统类型的不同而有所下降。当时，John Draper（“Captain Crnnch”）和Kevin Mitnick都在那儿。感谢William Knowles通过isn@securityforus.com的会议报道。

本书的设计既适于有多年Linux和UNIX使用经验的人，也适用于系统管理员新手，但前提是读者必须具有一定的系统管理员知识。

1.2 本书的组织结构

本书第一部分介绍如何提高系统的安全性。本书考虑到一些系统管理员只有很少的空余时间，却要在别人入侵系统时尽快修复各种严重的漏洞（较小的漏洞可以关闭，但一般来说，需要很长的时间进行定位。入侵者，有时被错误地称为黑客，是一些未经许可为获得乐趣、挑战

自我、获取名声等目的而侵入别人的计算机的人）。第2章“常见问题的快速解决”中介绍了这些可以立即解决的问题。这一章是从基本的安全概念的讨论开始，从而使一些Linux安全的新手快速成长，将经验丰富的人的知识进行一次刷新。作者根据有关“入口点”的报告和讨论，估计采用了这些方法可以使系统脆弱之处降低70%到90%。由于许多解决方法之间是相互独立的，所以系统管理员可以使用最合适的解决方法，并且可以按任何顺序来实现它们。

本书将进一步解决增强系统安全性的问题，允许系统管理员尽可能地将系统进行升级，甚至能寻址到内核并进行修改从而在更大程度上提高安全性。本书可以作为一本工具书，也可以作为一本参考书，其重要部分可从目录中找出。

第二部分介绍如何为非法入侵做好准备。没有哪个计算机或网络是绝对安全的。如果有人认为他的系统100%的安全，那么他也许还需要接受一些教育。大部分关于计算机安全的书总是专门地讲述安全系统而只用很少的页数来讨论对付入侵的问题，这样10%至40%的读者都会深受其害。我认为这只是天真的想法，因为其他所有常见平台更容易侵入。我对很多入侵情况做了分析：从黑客行为看来，系统的脆弱之处是软件系统中未被发现的bug，这就证明了仅仅保证一个系统的安全是不够的。

> 即使是最难应付的问题也有创新的解决方法，比如即使是Web服务器和整个Internet都瘫痪了，依然能够保证用户的信用卡号码的安全性，这涉及到与金融公司相关且波及面很广的问题。

本书之所以称为《Linux安全》，是因为在现实世界中，很多的计算机被侵入了。虽然有所准备的系统管理员早已做了很好的准备，但可能有5%至25%的处理Linux安全的系统管理员仍然要面对别人的进攻。即使是作者本人的基于PPP的动态IP站点也经常受到入侵的威胁。但我们已有所准备，所以即使是受到成功的入侵，也可以将系统迅速地恢复。

在我看来，切换到其他平台并不能减少这种风险。我看过很多关于在不同的成熟系统中发现安全性bug的问题。几乎每一周都会在长期运行和广泛使用的商业平台上发现容易忽视的脆弱之处。独立厂商所编的软件也有此类问题。

第三部分介绍如何监测入侵（包括正在尝试的和已成功的入侵），以及识别终端和登录的细节。第四部分讨论如何成功、完全、快速地进行恢复。这部分还包括跟踪黑客，以及起诉黑客或者用其他任何你想采取的措施对其进行惩罚。系统中断可能会导致一天几百万美元的损失，而不好的宣传意味着丢失更多的商机。再差一点，系统管理员的职位就保不了了，而恢复的速度快到无人知道时，系统管理员顶多只是在Internet上被人骂一顿。

本书介绍了许多安全问题，包括不正确的设置带来的问题，一些服务设计本身具有的不安全性，TCP／IP、UDP/IP、ICMP／IP、ARP和相关协议内部的限制，不同的Linux发行版本所带程序或安装到Linux系统上的程序中所含的bug，甚至于一些由于物理安全和人为原因（社会管理）而产生的问题。

不要认为Linux是一个设置困难、不值得注意和不够成熟，事实上Linux是一种很不错的操作系统。很多安全专家认为Linux和FreeBSD UNIX是最安全的常用操作系统，这是因为开放的源代码允许很多天才白帽子＇逐行检查代码并修改存在问题的地方，并将修改之处交给Linux维护

的主代码基地、自由软件基地和主要部分的开发者处。

在Linux和UNIX发布的不同BSD [2] 以及不同销售商提供的UNIX之间有大量的共享代码，这些代码对这些系统的所有用户都有好处，因为有更多的人可以改进其中的代码。通过依照本书上讲述的方法去做，即使一个专业的黑客也会被监测到，并可以用几分钟迅速恢复系统，而不是像毫无准备的白宫 [3]、伦敦的Lloyd、eBay.com [4] 等那样的站点需要花几天或几个小时的时间来恢复系统。

1.2.1 本书的约定

本书每章开头的内容列表可以用来快速地查找适用的内容。书后的附录涉及的内容非常广泛，而且许多条目都是基于子系统或涉及到的程序或程序类型来进行交叉参考的，比如脆弱之处。每节都列出了相应的Internet资源（URL），很多常用的Internet资源在附录A中会谈到，附录中也列出了很多URL，附录B讨论非Internet资源，包括书、CD-ROM、视频，有些可以免费索取，其他附录包括源代码或其他因过于庞大不宜在正文中出现的代码。本书附带的CD-ROM中也有这些内容，并且收录了文中讨论过的一些开放源代码工具。本书相应站点http://www.realworldlinuxsecurity.com上有这些内容，该站点上还包括最新的信息和勘误以及缩略术语库。

楷体内容是用来强调与话题相关的经验或开始有关讨论的，有时候它们着重指出一些特别重要或有趣的东西。

并没有很多人明白TCP/IP是一种在网际协议上的传输控制协议，这意味着到达的TCP／IP报文先被通信栈的IP层处理，然后才是TCP层，最后才被传到端口侦听程序。同样，UDP／IP是在IP上的用户数据报协议（UDP），ICMP／IP是在IP上的网际控制消息协议，这些可参见本书中有关TCP、UDP和ICMP的介绍内容。

1.2.2 背景

黑客同样具有从UNIX经销商、其他操作系统那里获得的源代码的拷贝，所以他们知道这些系统的脆弱之处。与Linux不同，对于UNIX而言，没有那么多白帽子致力于研究代码的缺陷并给予修正；而因为工作的自由，Linux的志愿者们是全世界的一些最好的程序员。他们的目标是最好的代码，而且不用受上市时间、开发经费及金融世界的其他限制。

这本书是为Linux系统管理员写的，但95%的内容可以应用到UNIX系统。主要区别是大多数UNIX系统管理员不能访问源代码，从而需要到经销商那里进行修正，大多数经销商能很快发布修改安全漏洞的措施，而且他们的客户也会提供有关的信息。有些安全问题是不同的服务和协议带来的，类似的问题也会出现在所有平台上，包括UNIX、Macs、Windows、VMS以及支持相同服务的其他平台上。

本书包括黑客的类型和目的、安全漏洞的类型和相应补救措施以及如何在网上找到最新的关于漏洞及其补救措施的消息。很多情况下，系统管理员也兼有其他职责，如网络管理员、数据库管理员、网站管理员、操作人员等，本书同样适用于他们。另外，写应用程序、CGI、

Shell脚本的程序员也应该了解怎样避免安全漏洞。

系统管理员确保用户了解安全方面的知识也是很重要的。因为一些安全漏洞需要对用户账户进行访问，所以一个用户的不具安全性的文件和程序可能导致他自己的数据、系统和网络的其他部分被入侵。

确保不存在非权威和未经分析的Internet与内部LAN或WAN（有时称之为Intranet）的连接也非常重要。写一个策略来保证安全虽然麻烦，却是很重要的一部分。如果写在纸上，人们很难忽视它。即使因为忽视它而产生了问题，也可以有理由责备失误者，本书有一整章是研究策略的。

Intranet被在其中传输的机密数据流认为是可信赖的，因此一旦连接系统不安全，黑客就可以从Internet潜入Intranet从而看到可靠数据并且有可能侵入重要系统。

1.3 需要防范的内容

必须防止以下几种情况的发生：

1) **黑客读到机密信息**。黑客可以看到你的产品设计、有竞争力的计划、客户的姓名和地址、客户的信用卡和银行账户信息、银行的账号数及内容和调制解调器呼叫的电话号码和密码等敏感系统信息。

如果黑客让别人使用这些数据会带来更大的害处。也许黑客本人知道产品设计并不严重，但如果把它放到网上让竞争对手看到，情况便严重了。如果你的客户的信用卡号码泄露了并被公开，人们将不会再与你进行交易。

2) **黑客修改你的数据**。这是最恐怖和有害的入侵，黑客可以不知不觉地改变设计和数据。这会带来生命和信誉的严重损失。如果一个药品公司的药品配方被改了，汽车或飞机的设计被改了，一个工厂的运作程序被改了，病人的X射线或γ射线仪器被改了，病人的医疗记录被替换了，会出现什么情况呢？任何一种情况发生都可能导致死亡，也会导致大的官司。

黑客可能并未意识到他的行为所带来的害处。加州的伯克利有一些黑客进入了一个对治疗癌症的回旋加速器进行控制的系统，黑客有时导致银行的ATM在没人时吐出钱，有时在机关（包括中央情报局）的网页上做令人尴尬的修改。

3) **黑客移除你的数据**。它的危害不言自明，如果能够检测到这种破坏，那么一个优秀的备份程序可以限制其带来的损害。

4) **拒绝服务**。这是当黑客导致计算机或网络不好用或不可用时产生的。不好用包括系统由于黑客的引入负载或重调度，合法用户可用的调制调器或端口减少（黑客关闭一些端口导致的）而引起的系统性能下降。不可用是指黑客导致系统崩溃或不能正常工作。

黑客可能会认为对一个控制电话交换的计算机进行攻击是很有趣的。但是，如果阻塞了911紧急呼叫，破坏了航空控制系统的话音和雷达电路在控制塔和远程无线电天线以及其他控制塔之间的连接，这可能会带来生命的损失。记住，在美国，干涉飞行物操作而带来生命损失时，做此干涉的人会处以死刑。

5) **黑客从你的站点发起其他攻击**。这会因为带宽损失和其他站点对你的站点进行封锁而引起服务的中止。这种攻击会带来不良声誉以及法律责任。

上面的任何攻击都会带来或大或小的问题，如一个公司的破产或系统管理员被解雇。当然，后者是最严重的。

1.4 谁是你的敌人

1. 黑客

通常，黑客认为他们所侵入的计算机的公司或机构是邪恶的或无关紧要的，而有时他们的行为却是友好的（因为他们没有破坏、公开机密数据或导致服务中止），但却使系统管理员浪费很多时间和金钱去找他们。有时他们的目的是造成尽可能大的麻烦，他们的攻击随机出现，但却专门攻击著名网站，尤其是著名公司或政府机构的站点。黑客往往很难被抓到。

通常他们用连接收费电话的便携式电脑接入。然后他们将从一个中介系统或通过一长串中介系统进入另一个中介系统，复杂的攻击使用一长串的中介系统，从而使跟踪和抓到他们变得复杂，甚至不可能。多年来，黑客周期性地张贴从中介处偷到的顾客的信用卡号。但自1999年以来，发生过很多黑客从太平洋电话等商家盗得大量信用卡并勒索几百万美元的事例，如果没有付钱，有效的卡号便被张贴出来，显然，其动机就是贪婪和偷窃。

有些人侵入其他系统只是为了有一个操作基地，从而进一步侵入其他系统。他们的目的是在这些基地系统上可以不被发现，除非系统管理员是非常警觉的，否则黑客可以在系统里待几个月甚至几年。他们利用这些系统得到一个难以跟踪的账户或利用它向其他计算机进行大量的分布式拒绝服务攻击，本书将介绍有效地监测这些“静态黑客”的技术。

2. 不满的现任职员

这些攻击也是难以预测的，但彻底审查可以发现他们，而且他们也会因害怕被抓到而减少攻击发生的可能性。经常备份并用不会丢失的方式进行存储是很重要的。

当然，如果拙劣的审查、遣责或不合意的任务分派将会给职员提供访问重要数据或硬件的机会，制作系统备份或改变用户访问代码等是谨慎的做法。

3. 不满的前任职员

假设被解雇的职员要做的第一件事就是破坏系统，那么这些攻击在某种程度上是可以预测的。大多数系统管理员需要做的枯燥工作之一就是当一些人与老板冲突被解雇时，取消他们访问计算机的权限。自然，赋予这些人访问权限的人会被通知终止这些权限，这包括拥有访问权限的经销商和其他职员。

这使我们想起以前的一个惨案，一位加州航空公司的职员被解雇，却没有人通知其他职员或安全人事部门，而航空公司职员不需要通过金属检则器。这位刚被解雇的职员利用这个便利将枪带到飞机上并枪杀了机组成员。飞机坠毁了，无人生还。所以安全是一种严肃的事情。

4. 竞争者

你的竞争者会尽力得到你的产品设计、客户名单、近期计划等信息，这些信息可用来盗窃你的设计、客户，有时还可将一些尴尬的事情公之于众。

并不完全是竞争者，猎头公司也会想尽办法获得雇员的名单和电话号码从而将他们“挖”走。有些公司将其职员名单和电话号码在网上公开，建议最好不要这样做，否则会成为别人的猎物。尽管你可能只是想张贴少数职员的名字和号码以便于对外联系。