Linux System Security

The Administrator's Guide to Open Source Security Tools

Second Edition

Linux 系统安全

—— 开放源码安全工具管理员指南

（第二版）

Scott Mann

[美] Ellen L. Mitchell 著

Mitchell Krell

周元兴 彭 成 池雅庆 等译

钱言琮 审校

電子工業出版社

Publishing House of Electronics Industry

http://www.phei.com.cn

Linux 系统安全

——开放源码安全工具管理员指南

（第二版）

Linux System Security

The Administrator's Guide to Open Source Security Tools

Second Edition

Scott Mann

[美] Ellen L. Mitchell 著

Mitchell Krell

周元兴 彭 成 池雅庆 等译

钱言琮 审校

電子工業出版社

Publishing House of Electronics Industry

北京 · BEIJING

内容简介

本书从安全性的角度介绍了Linux系统的安装、配置和维护。第1章至第4章概述性地介绍了系统的脆弱性、安全策略、密码技术以及网络互联，并且对用户账户、文件权限以及文件系统选项等方面的内容进行了研究；第7章和第8章主要阐述了系统账户管理和系统记录，它们在保护系统安全性方面发挥着重要的作用；第5章、第6章和第9章至第17章是本书的核心部分，这些章节描述了如何利用Linux系统特有的安全性和公开可获得的工具来增加系统的安全性；第18章则展示了如何执行本书所涉及到的所有应用工具。通过阅读本书，读者将会全面了解Linux系统的安全管理。

本书可以作为系统管理员在Linux系统上实施安全性措施以及使用安全性工具的指南，也可以作为研究Linux系统安全性的软硬件设计师和工程师的参考书。

版权贸易合同登记号　图字：01-2003-0598

图书在版编目（CIP）数据

Linux系统安全——开放源码安全工具管理员指南（第二版）/（美）曼（Mann, S.）等著；周元兴等译. -北京：电子工业出版社，2004.4

书名原文：Linux System Security: The Administrator's Guide to Open Source Security Tools, Second Edition

ISBN 7-5053-9626-9

Ⅰ.L...　Ⅱ.①曼...　②周...　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（2004）第004863号

责任编辑：赵红燕　王思斯

印　　刷：北京市增富印刷有限公司

出版发行：电子工业出版社

北京市海淀区万寿路173信箱　邮编：100036

经　　销：各地新华书店

开　　本：787 × 1092　1/16　　印张：33　字数：845千字

印　　次：2004年4月第1次印刷

定　　价：48.00元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换；若书店售缺，请与本社发行部联系。联系电话：（010）68279077。质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

译 者 序

Linux 作为一个开放式的操作系统，不可避免地存在一些安全隐患。随着 Linux 系统的广泛应用，如何排除这些隐患并为应用提供一个安全的操作平台成为亟待解决的技术问题。Linux 是开放式的系统，可以在网络上找到许多现成的程序和工具，这方便了用户，但也为黑客提供了方便，因为他们同样也能找到程序和工具来潜入 Linux 系统以达到盗取系统上重要信息的目的。不过，在充分了解 Linux 系统存在的安全隐患后，可以仔细设定 Linux 各种系统功能并添加必要的安全措施，这样就能够使黑客无可乘之机。基于此目的，本书深入系统地探讨了 Linux 操作系统中存在的各种安全问题，并讨论了 Linux 系统的安装、配置及维护等，因此可以成为系统管理员在 Linux 系统上实施安全性措施、使用安全性工具的操作指南。

本书首先概述性地介绍了 Linux 系统的脆弱性、安全策略、密码技术以及网络互联等一系列与 Linux 系统安全相关的主题，并且对用户账户、文件权限以及文件系统选项等内容进行了全面的研究。接下来，用两章的篇幅对系统账户管理和系统记录展开了详细的讨论，它们在保护 Linux 系统安全性方面起着极为关键的作用。此外，书中还深入探讨了如何充分利用 Linux 系统自身所具备的安全性，以及如何利用可公开获得的工具来增加安全性。最后，还讲解了书中所涉及到的应用工具在使用过程中的具体操作方法。

全书主要由周元兴、彭成、池雅庆翻译，并由钱言琮审校。参加翻译和译稿审阅的还有李蕾、徐东来、赵天磊、黄齐华、李根、李坡、傅冰、水心灏、饶翔、彭涛、林繁等。同时，本书还得到张志龙和司功闪的指导和帮助，在此表示感谢。

在翻译过程中，我们对原文个别错误做了更正。由于译者的水平和经验有限，错误与不妥之处在所难免，恳请读者批评指正。

前　言

我们的需求是本书存在的全部理由。从某些方面来说，我们真心希望其他人已经完成了这本书，这样直接拿过来读就可以了。我们在写作过程中深切体会到读一本书要比写一本书容易得多。

本书主要从安全性的角度介绍了 Linux 系统的安装、配置和维护。实际上，它可以作为系统管理员在 Linux 系统（所讨论的很多内容也能够适用于各种版本的 UNIX 系统）上实施安全性措施以及使用安全性工具的指南。我们相信本书能够为你今后维护系统安全的工作提供一个良好的开端。如果你采纳了本书中所阐述的操作流程，那么毫无疑问可以大大降低系统整体的脆弱性，并且使你拥有一个早期报警系统，它能够防止那些最为危险的系统和网络非法侵入事件的发生。

在本书中，类似密码技术、安全策略、TCP/IP 网络互联、防火墙等主题都有一些非常出色的资料可供参考，我们将在相关各章的最后部分以及附录 A 中提供这些主题的参考资料。此外，我们尽可能地为很多没有详细阐述的主题提供了类似的参考资料。

尽管书中也泛泛涉及到了一些黑客伎俩，但目的不是告诉你如何去非法侵入别人的系统，而是为了提高你防范它们的警觉性。本书所做的就是建立了一个基础框架，这将为你今后的深入学习提供很大的帮助。

关于本书

本书为你提供了一个可供遵循的操作规程，通过它能够更好地加强计算环境的安全性。此外，我们尽量让各章具有一定的独立性，在写作过程中我们始终贯彻这一原则。对于那些不知如何实现安全计算环境的读者，由于本书具有很好的完整性，通过阅读本书会从中受益匪浅，因此还可以把它当做是一本参考书籍。如果此前从未接触过安全性这一主题，请最好在阅读本书之前首先阅读“Practical UNIX and Internet Security”一书，或者其他类似的参考资料。

在本书中，我们包含了编译大多数应用程序的指令，之所以这样做（这些程序指令很快就会过期而失去价值），是因为尽管一些资源一般性地描述了建立软件的流程，但是很少提供真正的例子。根据我们的经验，只有很少新的或初级的系统和网络管理员有必要去获取一个公开可获得的工具，对该工具进行修改并成功编译它。正是为了这部分读者，我们才在书中包含了这些指令，而对于不需要这些指令的读者，只要跳过这些内容就可以了。

本书的前 4 章均为概述性的内容。第 1 章是一个关于脆弱性的调查，第 2 章介绍了安全策略这一至关重要的主题，第 3 章涉及到了从密码技术到网络互联等一系列的主题，这为本书随后的内容提供了一个框架。第 4 章主要对用户账户、文件权限以及文件系统选项等内容进行了全面的研究，因为这些内容均与安全性密切相关。

本书的第 7 章和第 8 章主要涉及了系统账户管理和系统记录这两个主题，它们在保护系统的安全性方面具有非常重要的作用，如果缺少了对这两个主题的讨论，那么这本关于系统安

全性的书籍将会是不完整的。第 5 章、第 6 章和第 9 章到第 17 章是本书的核心部分，这些章节详细阐述了如何利用 Linux 系统的安全性功能，以及如何采用那些公开可获得的工具来增加 Linux 系统的安全。在开始使用本书其他章节介绍的工具之前，一定要首先学习并在实际中使用 tiger 工具和 Tripwire 工具(参见第 14 章)。如果使用得当，这两个工具将会为系统提供一个关于安全性状况的很高置信级。

另外，第 18 章向你展示了如何去具体执行本书中涉及到的所有工具。如果你不能够详细阅读本书，那么在对系统安全性这一主题进行学习之前最好能够通读此章内容，这样能够了解在提供一个安全的环境前需要做些什么。

勘误

书中存在一些错误是在所难免的。尽管出于准确性的考虑，我们已经在 Red Hat 5.2 系统上测试了本书中所提供的每一项工具，在 Red Hat 6.0 系统上几乎也测试了每一项工具，但是毫无疑问在文中仍会存在一些错误。如果你发现了任何错误，请发送电子邮件将想要提出的批评和建议告诉我们，我们的邮箱地址为：

linux _ upat@thekeyboard.com

我们可能不会立即回复，但是会将更新和更正信息发送到下面的站点：

http://www.phptr.com/ptrbooks/ptr 0130158070.html

请经常查看这个站点以获取最新的信息。

第二版中的新内容

从我们第一次写作本书时起很多东西已经发生了变化，安全性在一个更为广泛的层次上被大多数的系统(包括 Linux 在内)所接受。在安装过程中建立一个防火墙、使 xinetd 成为默认的网络服务守护进程，以及在 CD-ROM 中附带了更多种类的安全工具等，都为获得一个更为安全的计算环境发挥了作用。当然，所有这些辅助功能都仍然建立在正确配置的基础上。

我们已经更新了几乎所有的章节，并且确保本书介绍的所有内容均能够与 Red Hat 7.2/7.3 系统兼容。此外，我们还加入了两章新的内容，其中一章介绍 iptables(参见第 16 章)，而另一章则讨论了网络扫描程序、嗅探程序以及探测程序(参见第 17 章)。一些较旧的材料，譬如 OPIE(参见附录 C)、TCP _ wrappers(参见附录 D)和加密文件系统(参见附录 E)都已经放到了附录中。这些仍然是有用的信息，但是通常情况下使用的机会较少。所有其他各章仍然涵盖与以前相同的主题。

我们希望本书对你们能够有所帮助。

Scott Mann 的致谢

写作这本书是一次极不寻常的旅程，我有幸结识了很多对我一生都具有重大意义的人，并且还从我的朋友那里获得了大量极为宝贵的支持。因此，我要对下列这些人表达诚挚的谢意。

我要感谢 Mary Franz 和 Noreen Regina，以及 Prentice Hall 所有支持这一项目的工作人员。

他们为本书的出版付出了很多的努力。

Radia Perlman 为这个项目提供了大量的支持，正是因为 Radia 中肯的意见才使得本书的质量能够更上一层楼。此外，Todd O'Boyle 发现了很多我容易忽视的问题。Tom 给出了很多有用的批评和建议。感谢你们所有的人！

Ellen L. Mitchell 重新审查了本书，她检验了很多例子，并指出了许多程序错误。我邀请她帮助我完成这本书，在她的帮助下这本书才能够与读者们见面。感谢你，Ellen！

Sue Finnegan 曾经有一天对我说："你真应该去写一本书。"这样我就知道接下来应该做什么了。谢谢你，Sue，为了整件事情由你而起也为了我们多年来的友谊。

还要特别感谢 Mark Wright，Bruce Robb，Mike Look 和 Sharon Dean，他们自始至终支持这个项目并提出了合理的建议。

感谢我的家人，感谢他们给予的支持，我的父母 Richard 和 Julie Mann，姐姐 Lisa，妻子 Connie，还有我的孩子们 Melissa，Joshua 和 Christiana。我能够取得今天的成功，离不开他们的支持。

此外，还要把特别的感谢送给那些响应我的电子邮件、新闻组帖子的朋友们。尤其感谢 Tom Dunigan 告诉我关于编译 CFS 1.4.0 beta2 版的技巧，Aniello Del Sorbo 提供了关于 TCFS 的帮助，Rob Braun 回复了我提出的关于 xinetd 的问题，Craig Metz 提供了关于 OPIE 的信息。还要感谢 David A. Ranch 所有关于 ipchains 的反馈。

最后，把我最真诚的感激献给 Anita Booker，盼望我们之间的友谊能够天长地久。

目　录

第 1 章　系统脆弱性调查

在一个深夜。

“看啊，这是一个足以向世界发布的消息！我所需要做的仅仅是获得一个有效的用户账户。”aBl _ tR3kr 大声说道。

“是什么值得向世界发布？”pl3b 问道。

“这个位于 windfall.naive.com 上的主目录。”

“windfall？”pl3b 接着问道。

“对，它马上就会成为我们的 windfall（意外之财）了！”

“究竟是怎么回事？”pl3b 继续询问。

“是这样的，”aBl _ tR3kr 笑着说道，“如果他们都愚蠢到了允许 NFS 位于 Internet 上的地步，那么他们也就有可能没有使用阴影文件（shadow file）。”

“阴影文件？”此时 pl3b 真正陷入了困惑中。

“是的。我所要做的就是在我的 Linux 机器上创建一个与他们账户的其中之一相符合的账户。好，有一个叫做 joe 的用户。”aBl _ tR3kr 在键盘上迅速地敲下这些字母。“现在我要作为 joe 在这里登录，那么显而易见我就可以从 windfall.naive.com 上获得 joe 的主目录了！”

“这真是太容易了！”pl3b 考虑着侵入 UNIX/Linux 系统不过是件简单的事情。

“现在我要创建这个 .rhosts 文件，接着我们就可以远程登录了。”aBl _ tR3kr 一边工作一边进行着解释。“好，我们已经作为 joe 进入了。现在让我来检查口令文件，太好了，没有阴影文件！我要将这个口令文件通过电子邮件发送回我这里，就像这样，完成！”

“那个文件有这么重要吗？所有的口令都是杂乱无章的。”pl3b 说道。

“没问题，我们可以对它进行破解！”aBl _ tR3kr 自信地微笑着。又一个系统落入了他的掌握之中。

注意：提供这段对话是出于说明的目的，它确实代表了一类非常严重的账户盗用问题。尤其值得注意的是，一旦获得了无特权的访问，那么就可以用多种方法进行目录访问。我们明确禁止这种行为。此外，拥有一些切身的感受对防止各种不利情况的发生也是极为重要的。我们鼓励出于预防目的而对使用中存在的各种脆弱环节进行研究。要想进一步了解有关常用系统和网络盗用方面的信息，可以从附录 A 提供的参考资料中获得。

1.1　系统存在的问题

这段对话体现出了可以对 Internet 系统进行未经授权访问的错误配置服务。这种情况的发生是极为普遍的，这在第 2 章中将会说明。

系统 windfall.naive.com 存在的第一个问题在于用户主目录是通过网络文件系统（Network File System，NFS）输出到外界的。如果采取保护措施，可以通过采用 ipchains 或 iptables（将在

第 15 章和第 16 章中分别进行介绍)工具(最好是将这两者结合起来使用),对 NFS 资源(将在第 3 章中具体讨论)和 portmap 应用工具(将在附录 D 中具体讨论)设置访问限制,这样做可以防止这类情况的发生。

前面提到的破解者 aBl _ tR3kr 在这一事件中还利用了可信主机文件(trusted host file).rhosts 来实现对该系统的未经授权访问。通过使用.rhosts 文件,aBl _ tR3kr 就能以用户 joe 的身份无须任何口令便登录进入 windfall.naive.com。我们将会在第 3 章中谈论到这些文件,并且会建议禁止使用它们。此外我们还将在第 11 章中讨论如何安全地替换这些文件。

系统 windfall.naive.com 存在的另一个问题就是它没有使用口令保护(将在第 4 章中具体阐述)。在这次侵入事件中,缺乏口令保护意味着有一个所有人都能读懂的文件(/etc/passwd),其中包含了每个用户的散列化(有时又称做"加密的")口令,任何一位能够访问一个用户账户的人都可以轻易获得这个文件,而 aBl _ tR3kr 恰好能够做到这一点。如果当时使用了阴影文件,那么 aBl _ tR3kr 就不可能如此轻松地获得加密口令表,因为阴影文件只有对根用户才是可读的。

尽管加密口令不能直接用来进行登录,但是基于这些散列口令,可以使用 Crack 破解程序(将会在第 12 章中详细介绍)猜出真正的口令。而且 Crack 破解工具在这一方面相当管用。你不可能防止坏人使用类似 Crack 这样的破解工具,但却可以交替采用一些不同的散列方法来增加破解口令工作的难度,这一部分的内容将在第 5 章中描述。

1.1.1 其他的黑客行为

一旦某个侵入者成功实现了对某个账户的访问,那么该侵入者将有可能去完成一系列的事情。而一个恶意侵入者肯定要去做的一件事情就是创建一个后门以便轻易地逃脱,该侵入者还会清除一切有关其行为的证据。目前有很多可以轻易获得的应用工具,通过它们可以非常简单地完成以上的事情。

本书为读者提供一些有效的方法,采取这些方法可以增加最初黑客侵入的难度,并且还能够迅速地侦测出黑客攻击的证据线索。但是本书不能作为你获取这方面信息的惟一来源。每次新出现的脆弱性问题都是不同的,所以也就会产生相应的补丁和修复程序。此外,考虑到计算机安全场景的变化,完全解密站点(在本章末尾的 1.5 节中将会加以注解)、电子邮件邮寄名单和新闻组还将会提供一些额外的细节内容。附录 A 列出了一些对你有所帮助的资源。

1.2 本书的目的

本章开篇的那段对话是为了说明那些经常发生的系统侵入行为类型。本书的意图是将众多的技巧、知识和工具提供给你,它们会在你并不了解究竟是谁正在访问什么内容的情况下,帮助你更好地设置系统以应付这些情况。书中所介绍的技术着重于限制授权访问的使用,并且尽可能地增加系统侵入者获得未经授权访问的难度。

本书将会介绍各种不同实用工具的使用方法,以便利用这些工具来更好地保护系统环境。尽管我们在全书中给予了很多的建议,但任何东西也代替不了采用一个行之有效的组织安全策略(将在第 2 章中具体讨论)。除此之外,如果你希望进一步了解我们所讨论的各个主题,我们还在每章的最后提供了一些参考资料以供查阅。

在详细介绍如何利用一些公开的工具以帮助你增强 Linux[①] 系统安全性之前，我们将利用本章的剩余篇幅来介绍当今普遍存在的系统薄弱环节和攻击类型。我们不会详细讲述它们究竟是如何工作的，但会定义出它们所具有的特征，以便你能够了解它们。此外还可以查阅 1.5 节找到更多的有关信息。

1.3　关于系统脆弱性和攻击性的调查

我们分别从技术、社会和物理这三个不同的范畴来讨论系统脆弱性。系统攻击者将很有可能利用这些范畴中的一个或多个系统脆弱性。

1.3.1　技术范畴

针对我们在计算机中所采用的技术，目前存在着多种攻击类型。其中的一些攻击通过对程序、脚本或数据的修改来达到目的，而其他一些则使用了某些特别技术。下面的内容便概括总结出了一些常见的攻击类型项目，它们描述出了利用计算机技术来进行的攻击。

特洛伊木马：隐藏的程序或脚本，通常情况下被嵌入到一段合法的程序或脚本中，这样，在合法的程序或脚本执行时，会出现未经授权的行为。在“Practical UNIX and Internet Security”一书中便记载了一个将特洛伊木马或后门嵌入隐藏到一个 C 编译器内的实例。这种类型的攻击是难以防止的，第 3 章中叙述了降低这种类型攻击发生的多种途径。尤其是在第 3 章中还介绍了验证校验和以及具有极好保密性（Pretty Good Privacy，PGP）的签名，这些在全书都会经常提到。

口令破解：猜出口令或者利用像 Crack 这样的工具来帮助猜出口令。在全书中，多次讨论了如何降低与口令相关联问题的危害性，尤其是在第 4 章至第 6 章和第 11 章中。

文件许可和路径设置：这两者中任何一个设置不正确都有可能导致系统遭受损害，对这一主题进一步的讨论将在第 4 章中进行。

SUID 脚本和程序：该脚本和程序在运行过程中会将真实或有效的用户标识符（UID）设置传送给调用该脚本和程序的用户以外的某人。通常情况下，我们主要关心的是设置根用户 UID（SUID）的程序。大量将无特权用户变为根用户的侵入事实都利用了这一机制。与此类似，另一些较少的侵入事实利用了集合组标识符（SGID）。我们将会在第 4 章中介绍这些问题。

可信主机文件：可信主机文件的使用经常会造成某个系统传播扩散到整个网络。在第 3 章中将会介绍这些文件。我们还会在第 11 章中讨论这些文件的替换功能。

缓冲区溢出：当未能成功限制一个程序中的读缓冲区时，有可能导致通过写入由读缓冲区定位的系统内存而实现对系统的侵入占用。尽管编写一个程序来利用不受限制的缓冲区相当困难，并且需要有特别的技巧，但是目前在 Internet 上可以获得很多由技术娴熟的人员编写的现成程序。我们将会在 3.8.2 节中更进一步地了解如何减少这类问题的发生。

扫描与嗅探：通过网络扫描，网络攻击者可以辨识出某个特定系统上所运行的操作系统（OS）以及可供利用的网络守护进程。网络嗅探则可以帮助黑客们获取机密的信息。网络扫

① 本书中所讨论的大部分内容均与商业 UNIX 平台相关。

描与嗅探对于安全测试和调试也是非常有用的。我们将在第 3 章和第 17 章中介绍一些用于此种目的的工具，在第 10 章和第 17 章中则会告诉读者一些降低利用网络扫描器进行攻击所造成的影响的途径，而在第 11 章和第 15 章中还会讲述一些减弱利用网络嗅探进行攻击所造成的影响的途径。

电子欺骗：某个用户伪装成另一个用户，某个主机(host)伪装成另一个主机，某个 Internet 协议(IP)地址伪装成另一个 IP 地址[①]，某个域伪装成另一个域或地址，所有这些都是电子欺骗的例子。这些类型的攻击以及如何降低它们发生的可能性在 1.5 节中所引用的“Hacker Proof”和“Maximum Security”两本书中都有极为详尽的论述。我们将会在第 15 章中介绍减轻这些类型攻击的途径。

TCP/IP 攻击：利用传输控制协议(TCP)网络连接的工作方式，有可能带来很多种不同的攻击方式，而且这些类型的攻击难于防止和侦测。我们在第 10 章、第 11 章和第 15 章中讨论的很多技术都可以用来降低这一类的攻击。此外，你还可以通过查阅 1.5 节中的“Hacker Proof”一书获取更多有关 TCP/IP 攻击以及如何去防止这类攻击的详细内容。

话路拦截：某个用户获取某个网络话路或连接的控制权。这是 TCP/IP 远端同步攻击的一种特殊情况，参见上面的“TCP/IP 攻击”。

拒绝服务：任何阻止正常使用系统和网络资源的行为都认为是一种拒绝服务(Denial of Service，DoS)行为。通常，你能够让 DoS 攻击对于网络犯罪者变得很困难，但是你却无法阻止 DoS 攻击的发生。在第 10 章中，我们将会介绍用 xinetd 替换 inetd，该程序可以防止某些与网络相关的 DoS 攻击。

其他薄弱环节：在各种不同的网络和系统应用程序中也存在着很多的薄弱环节，其中的一些将会在本书中加以讨论。如果你希望获取应用程序中存在的薄弱环节的进一步信息，那么可以参见附录 A。我们还在 1.5 节中提供了一些信息资源。

1.3.2 社会范畴

在所有安全策略(参见第 2 章)之中，最薄弱的环节就是被授权使用计算环境的人员。通过攻击这一薄弱环节来蓄意损害某个计算环境的人会利用人际交往。在安全性的所有方面之中，这一方面是最难加以控制的。尽管这方面的安全性已经超出了本书讨论的范围，但我们还是给出了一些常见的人际交往攻击类型，并在 1.5 节提供了一些常用的有关安全性的参考站点。

肩膀窥视(Shoulder Surfing)：顾名思义，就是通过在某人身后进行窥视获取某些敏感信息的行为，譬如某个用户的口令。

仿造：通过这类的人际交往攻击可以获得一些敏感信息。具体的例子包括假装成一个系统管理员或者自称是某个组织的高层官员，以便从该组织中不够谨慎的员工那里获取所需的敏感信息。

1.3.3 物理范畴

正如人们常说的，一旦物理安全性遭受破坏，那么一切也就无法挽回了。这种说法反映了

① 同样地，如果坏人使用了电子欺骗，那么可以看一下第 15 章所讲的伪装。

这样一个事实，那就是如果某个未经授权的人获得了对计算机系统的某个部分进行物理访问的权限，那么所有的技术性安全解决方案都无法阻止这个人的攻击破坏行为。对于这一主题本书也不会进行研究，但我们还是列出了一些潜在的薄弱环节。在国际信息系统安全认证社团[(ISC)²]的主页上可以找到有关这方面的内容。

系统访问：一旦有人实现了对某台计算机的物理访问，那么无论是以单用户模式启动该系统(参见 3.2.1 节中有关限制单用户模式访问的内容)，还是携带该系统都将成为可能。强烈建议从物理上限制对最关键系统的访问。

网络问题：网络的组建一般都是建立在以电为基础的媒介之上，比如 10/100 baseT 以太网、音频(RF)通信、微波技术和卫星通信。所有的这些通信形式都可以通过各种抽头技术(tapping technique)[①] 进行中途拦截。光纤媒介的使用很大程度地缓解了这一问题。参见 1.5 节中推荐的(ISC)² 站点主页可以获得更多有关该主题的信息。

其他的物理访问问题：在现实生活中存在着相当多的与未经授权物理访问相关的系统脆弱性问题，参见 1.5 节中推荐的(ISC)² 站点主页可以获得更多有关该主题的信息。

1.4　小结

本章概要介绍了一系列与计算机和网络相关的脆弱性问题和侵入破坏问题。尽管以上并非本书的重点，但本章却引出了安全系统需求这一话题，而这正是本书的重点所在。同时，我们还为更进一步的深入研究提供了数量可观的参考资料。

1.5　参考资料

参考书籍

Anonymous. *Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network*. Indianapolis, IN: Sams.net Publishing, 1997.

Atkins, Derek, et al. *Internet Security: A Professional Reference*, Indianapolis, IN: New Riders Publishing, 1996.

Barret, Daniel J. *Bandits on the Information Superhighway*. Sebastopol, CA: O'Reilly & Associates, 1996.

Chapman, D. Brent, and Elizabeth D. Zwicky. *Building Internet Firewalls*. Sebastopol, CA: O'Reilly & Associates, 1995.

Cheswick, William R., and Steven M. Bellovin. *Firewalls and Internet Security: Repelling the Wily Hacker*. Reading, MA.: Addison-Wesley, 1994.

Cooper, Frederic J., et al. *Implementing Internet Security*. Indianapolis, IN: New Riders Publishing, 1995.

Denning, Dorothy E. *Information Warfare and Security*. New York, NY: Addison-

① Newt Gingrich 通过大量的研究发现了这种技术。