新世纪网络工程师丛书

Linux 系统安全实用手册

Linux System Security

[美] Scott Mann & Ellen L.Mitchell 著

林雪梅 陆明俊 张润清 译

李卫国 校

電子工業出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 提 要

本书详细介绍了 Linux 系统的安全漏洞、防范策略以及常用安全工具的正确使用等内容。书中提供了大量的使用实例和使用技术细节，是一本网络系统安全、操作系统安全使用方面实用性很强的书籍。利用书中提供的信息，读者可以在 Linux 系统中制定出有效的安全措施来保障系统的安全。

所有实例，均在随书所附软盘中。

图书在版编目(CIP)数据

Linux 系统安全实用手册/(美)马恩(Mann,A.)、(美)米切尔(Mitchell,E.L.)著；林雪梅等译.

–北京：电子工业出版社 2000

(新世纪网络工程师丛书)

ISBN 7-5053-6162-7

Ⅰ.L… Ⅱ.①马…②米…③林… Ⅲ.Linux 操作系统–安全技术–手册 Ⅳ.TP316.89-62

中国版本图书馆 CIP 数据核字(2000)第 69125 号

丛 书 名：新世纪网络工程师
书　　名：**Linux 系统安全实用手册(附实例软盘)**
原 书 名：**Linux System Security**
著　　者：[美] Scott Mann & Ellen L.Mitchell 著
译　　者：林雪梅　陆明俊　张润清
校　　者：李卫国
责任编辑：陆伯雄
印 刷 者：北京天竺颖华印刷厂
出版发行：电子工业出版社　URL:http://www.phei.com.cn
　　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：31.25　字数：609 千字
版　　次：2000 年 8 月第 1 版　2000 年 8 月第 1 次印刷
定　　价：56.00 元
书　　号：ISBN 7-5053-6162-7/TP・3302

著作权合同登记号　图字：01-2000-0091

前　言

本书是适应人们的需要而出版的。从多方面得知，人们一直期望有人写一本有关这方面的书以供阅读。但是，写要比读难得多。

这本书从安全的角度介绍了如何安装、配置和维护 Linux 系统。事实上，这是一本在 Linux 系统上实施安全与使用安全工具的管理员指南(其中讨论的大部分内容也适用于各种 UNIX 版本)。这不是一本有关安全方面的权威书籍(也没有这样的书)，只是为确保与维护安全系统提供合理的基点。如果能够遵循书中的安全程序，就能减少整个系统的漏洞，及早警示系统以防止系统与网络受到破坏。

本书尽量避免重复讨论在其他书籍中已经详细讨论过的主题，例如：密码学、安全策略、传输控制协议/互联网协议(TCP/IP)网络、防火墙等等。本书会在合适的章节末尾以及附录 A 中指明这些主题的资料出处，并对许多来不及论述的主题也提供类似的资料出处。

本书的目的是提高人们的安全意识，但无意攻入他人系统，对系统处理以及漏洞评估的编码审计不加以论述，这种工作留待于更勤勉的人们来做。简单地说，本书是为希望在计算机安全领域有所作为的人们提供一个框架和基础。

关于这本书

本书目的是讲述如何遵循一个规则(你认为合理的修改)以确保更安全的计算环境。本书也确实是按照这种方式进行写作的。对于不熟悉如何实施计算安全环境的人们来说，将会从本书中获益。如果读者确实对安全很陌生，请先阅读 *Practical UNIX and Internet Security*《实用 UNIX 和互联网安全》或有关方面的书籍，然后再阅读本书。

本书还提供最实用例证指南，这是因为在许多书籍和资料中只概括介绍创建软件的过程，却很少有实用的例子。根据作者多年的经验，新手或系统与网络初级管理员对如何获得有用的开放工具以及正确修改与成功编译这些工具缺乏必要了解。当然，如果不需要这些指南可以略过不读。

前 4 章是对本书总的概括；第 1 章是对安全漏洞的概括，第 2 章介绍了安全策略的重要问题，第 3 章论述了密码学到互联网主题框架的有关问题，第 4 章概要介绍了用户帐号，文件许可权限，文件系统选择等与安全有关的主题。

第 7 章与第 8 章分别论述了系统帐号与登录系统的问题，如果一本有关系统安全的书籍没有论述以上这些主题的话，不能算是完整的。第 5 章、第 6 章和第 9 章到第 17 章是本书的核心，详尽论述了如何利用 Linux 的安全防范能力以及使用公开有效工具加强 Linux 安

全的问题。在使用本书论述的任何一种工具之前，请先学习与实践 tiger(第 13 章)和 Tripwire(第 14 章)。这两种实例能够大大加强人们对系统安全的信心，当然必须使用得当。

第 18 章将讲述如何实施书中论述的所有安全策略。如果你认为时间仓促，在学习某一主题时，先通读该章，以便了解如何获得一个安全环境信息。

真诚希望本书对读者有帮助！

有关勘误表

错误当然会有，在本书中尽管对红帽子(RadHat)5.2 和 6.0 版本的一切问题进行了校验，但在文本中难免会出现错误。如果读者发现了错误或想发表评论时，请 e-mail 给如下地址：

linux_upat@thekeyboard.com

也许不能及时答复读者的 e-mail，但会在 http://www.phptr.com/ptrbooks/ptr0130158070.html 上刷新并更正。

请有空浏览一下网站新内容。

Scott Mann 致谢

写这本书是一次不同寻常的经历，认识了许多改变我生活的人们，这给我带来了乐趣，同时也得到了朋友以及相识人们的鼎力支持，在此我要对以下人员致以诚挚的谢意。

Mary Franz 是一名出色的编辑(确实是一位老编辑，但她并不老)。她回复了我所有电话以及一些可笑的问题，她甚至在工作的重压下，还要倾听我的学术论题。感谢 Mary 希望这本书不会令她失望。

在写书初期，Mary 约我与 Camille Trentacoste 见面，他确实是编辑写作与 FrameMaker(排版软件)的行家，Camille 讲述了十分钟有关 FrameMaker 知识,这要比我十年学到的东西还多(当然，我从没读过这方面的手册)。感谢 Camille。

感谢 Noreen Regina 欣然为我校稿，同时也对支持我写书的同僚们表示感谢，有许多人我从来就不认识，通过 Mary，我知道了他们。

Radia Perlman 为此书付出了巨大努力，她对本书的评论是无价的，热情是无限的。她的精辟见解使本书奕奕生辉。Todd O'Boyle 同样也作出了巨大努力，他阐明了一些我容易忽略的问题。Tom Daniels 也提供了不少支持，提供了大量有用评论。感谢你们！

Ellen L.Mitchell 对本书进行了校稿，她验证了许多例子并指出了大量漏洞。我要求她与我一道完成这本书，她在一边工作一边修读博士学位的同时，帮我完成了这项工作。Ellen，可以这样说，没有你的帮助，这本书是不会完成的。

Sue Finnegan 有一天对我说，“你确实应该写一本书了”，接下来的是，我得到了 Mary Franz 答复，感谢 Sue 使工作顺利开展以及多年的友谊。

如果说有人对本书的贡献功勋卓著的话，当推 Mark Wright，他是一个老道的技术专家，

难以置信地追求完善，是一个具有远见卓识的人，感谢 Mark 的全力支持及友谊。

特别感谢 Bruce Robb，其法律建议也是难以估价的。

最诚挚感谢 Mike Cook, 其巨大热情促使工作顺利地完成。Sharon Dean 同样也付出巨大努力。

我还要感谢我的家人，我的父母 Richard 和 Julie Mann，我的姐姐 Lisa，我的岳母 Susie Cook 和妻儿们。我想现在有空与孩子们一起玩了。

特别感谢答复 e-mail 的朋友，特别是，感谢 Tom Dunigan 提供编辑 CFS Version 1.4.0beta2 的技巧，感谢 Aniello Del Sorbo 帮助编辑 TCFS，感谢 Rob Braun 解答 xinetd 问题，感谢 Craig metz 提供有关 OPIE 信息，特别感谢 David A.Ranch 对 ipchains 问题的反馈。

最后，向理解和支持我完成这项工作的 Amita Booker 致以最崇高的敬意，希望我们的友谊永存。

Ellen L.Mitchell 致谢

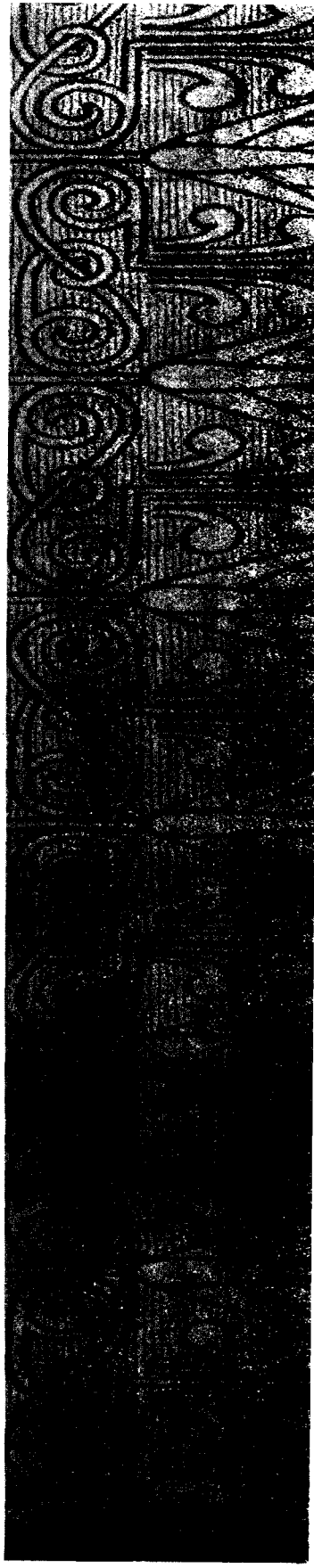
首先，我要感谢 Scott Mann 先生给我这次工作机会，此项工程是巨大的，对于 Scott Mann 先生来说尤其如此。我从没听他抱怨过一次，Scott 先生，与你一起工作是多么的快乐。

感谢 Noreen Regina 的努力工作，使其得以按时完成。感谢从未谋面的其他参予这项工作的人们。

感谢 E.Todd Atkins 及时为我解答有关 swatch 问题。

特别感谢 Douglas Schales 和 David K.Hess，二位是 tiger 的原创作家，他们耐心地解答了许多问题并校对了一些写作材料。感谢他们的付出与友谊。

最后感谢我的朋友们和合作者的支持与友谊。



第 1 章

漏洞概述

深夜……

“看！一切都可得到，我所做的就是获得一个有效帐号”，aBl_tR3kr(发音“able trekker”)大声喊道。

“你说什么？”吃着巧克力豆的 pl3b(发音“plebe”)问道。

“就是在 windfall.naive.com 上的主目录”。

“windfall？”pl3b 问道。

“是的，一会儿将成为我们的 windfall 了！”

“你怎么做？”pl3b 问道，他想知道更多的东西。

“啊，”aBl_tR3kr 笑着说，“如果他们愚蠢的话，会让我们在互联网上获得 NFS，这说明他们很可能没用影像(shadow)文件。”

“影像文件？”pl3b 显出非常困惑的样子。

“是的，就是在我的 Linux 信箱里创建与其中一个帐号相匹配的一个用户帐号，当然，有个用户叫 Joe”aBl_tR3kr 迅速地键入 Joe，pl3b 顺着望去。“现在以用户名 joe 登录，从 windfall.naive.com 上得到了 Joe 的主目录！”

“哇，好简单啊！”pl3b 想道，原来进入 UNIX/Linux 系统如此容易。

“现在，创建.rhosts 文件，将远程登录。”aBl_tR3kr 边说边工作，“好，以 Joe 身份进入了，现在，检查口令文件，哇，没有影像文件！我只需用 e-mail 向自己发回这一口令文件，完成了！”

“发这样的文件有什么好处？所有的口令都在一起，”pl3b 说道。

“没问题，我亲爱的朋友，我们只是使用了 Crack！”aBl_tR3kr 自信地笑着，另一系统已落入其掌握之中。

注释：

这段对话的目的是举例说明这是一起严重的利用漏洞入侵事件。并不是一起典型的入侵行为，也不代表与未授权访问用户帐号有关的所有潜在入侵事件。需要特别指出的是，一旦获得未授权访问，就有获得根访问的许多方法。本书严正指出不支持这种行为。然而重要的是，了解这些入侵行为会更好地防止入侵。本书支持读者以预防的目的来学习各种漏洞。在附录 A 中有一般系统和网络入侵更多的信息。

1.1 发生了什么？

上面的对话介绍了未授权访问互联网系统的漏洞系统服务，这种实例将在第 2 章中经常出现。windfall.naive.com 系统出现的首要问题是，通过网络文件系统(NFS)可对外输出用

户主目录，可通过 ipchains(第 16 章有述)对 NFS 资源(3.5.4 节“一些主要的应用程序”中有论述)以及对 portmap 工具(第 10 章有述)设定访问权限可防止这一问题的发生。

快乐的黑客 aBl_tR3kr 也利用可信任的主机文件.rhosts 获得对系统的未授权访问。在对话中，ABl_tR3kr 利用.rhosts 文件以 Joe 的身份(没有口令)登录到 windfall.naive.com。在第 3 章中将论述这些文件以及如何防止入侵的方法。在第 11 章将论述如何安全替代这些文件。

Windfall.naive.com 系统出现的第 2 个问题是，不使用影像口令(4.1.3 节“口令有效期与影像文件”中有述)。在这一实例中，非影像口令意味着获得有效用户帐号的人可读取包括所有用户 hashed(有时指“加密”)口令在内的可读文件(/etc/passwd)，aBl_tR3kr 就获得了这样的帐号。如果使用影像文件，就不能轻易地得到加密(hashed)口令，因为影像文件只有在根用户下可读。

由于加密口令不能用于登录，可使用 Crack 工具(第 12 章详述)猜测加密口令，Crack 工具在猜测口令方面是相当不错的，但不能防止黑客利用此工具，但可使用不断变换加密口令(第 5 章有述)的方法使黑客难以入侵。

1.1.1 其他黑客活动

一旦入侵者获得帐号就会有机可乘，恶意入侵者几乎确定要做的事就是为其返回创建一个后门。入侵者还将掩盖其活动痕迹，有许多免费工具使这一活动变得轻而易举。

本书的目的就是提供多种途径阻止初次入侵并很快发现入侵证据。但并不是说本书或其他一些书籍提供的方法是防止入侵的唯一手段。新的漏洞总是会不断发现，相应的补丁也会随时发布。同时，全面发布网站(1.5.4 节“全面发布资源”中有述)、e-mail 列表和新闻组都将提供计算机安全变化的详细内容。列表资源将会为你随时刷新信息。

1.2 是否准备演示如何入侵系统

否。

本章最初的对话是列举一些经常发生的入侵事件。本书的目的是为读者提供安全技术、知识和工具以防备入侵系统，从限制授权访问的角度来论述各种技术与方法，因而入侵者难以获得未授权访问。

本书论述的是安全基础知识，因此，会讲述各种保护系统环境的方法，至于如何实施系统安全将留待于其他的安全资源论述。本书将推荐好的有组织性的安全策略，同时，如果有兴趣进一步探讨某一主题时，在每一章的结尾列有参考资源，会进一步讲述如何维护良好的安全系统。

在详细论述使用开放安全工具保护 Linux[①]系统之前，本章剩余部分将探讨当今普遍存在的各种漏洞和进攻，但并不详述其入侵过程，只是对其特点加以定义，使读者有个更好的理解，详细内容请参见 1.5 节“深入阅读资料”。

1.3 漏洞与入侵概述

从技术、社会以及物理范畴探讨漏洞，入侵者试图从这些范畴利用漏洞。

1.3.1 技术范畴

有许多利用技术进行入侵的行为，有些是通过修改程序或脚本或数据进行入侵的，有些是利用特殊的技术进行的，下面概括了一些入侵的普通术语。

特洛伊木马 特洛伊木马，即当执行授权程序或脚本时，嵌入于授权程序或脚本中，进行未授权活动的隐含程序或脚本。*Practical UNIX and Internet Security* 一书的 801-802 页 Trusting Trust 中对隐含在 C 语言编译器的特洛伊木马或后门案例进行了分析，这种入侵方式是很难防备的。第 3 章全面讲述了如何降低这种入侵风险，特别论述了对包含特洛伊木马的文件验证求校验和及 Pretty Good Privacy(PGP)文件签名，本书的其他章节对这些问题也将有论述。

后门 后门指的是，嵌入于普通程序或脚本中，对系统进行未授权访问的隐含程序和脚本，类似于特洛伊木马。

破解口令 猜测口令或利用 Crack 工具猜测口令。防止破解口令的方法论述贯穿于本书，特别是在第 4，5，6 和 11 章中都有论述。

文件许可权限及路径设置 其中任何一种不当的设置都会造成入侵系统，在第 4 章中有详细论述。

SUID 脚本和程序 与真实或有效的用户标识符(UID)运行在一起的脚本或程序，该用户标识符设置为不是调用这一脚本或程序的用户。通常，令人不安的是 UID 设置为根用户的程序，许多入侵就是允许未授权用户成为根用户，利用的就是这一机制，但很少有利用组标识符(SGID)的入侵活动，第 4 章将对这些问题进行论述。

可信主机 使用可信主机文件，利用一种系统入侵整个网络的入侵方法(第 3 章对可信主机文件有述)。第 11 章论述了这些文件的代替功能函数(functionality)。

缓冲区溢出 由于程序中的读缓冲区有限，通过写入由读缓冲区分配的系统内存使系统受到入侵。很难找到足够大的缓冲区写程序，因此需要特殊的技术，在互联网中有许多用这种技术写的程序。第 3 章 3.8.2 节“测试软件”中有详细论述。

---

① 本书论述的大部分 Linux 系统与商业上使用的 UNIX 平台有关。

扫描与嗅探 入侵者利用网络扫描方法，识别运行特殊系统及网络守护程序的操作系统(OS)，入侵者还可以通过网络嗅探以获得机密信息。扫描与嗅探网络能有效测试安全及排除故障。第 3 章和第 16 章讲述了一些有用的工具。第 10 章和第 16 章讲述了利用网络扫描仪减少入侵的各种方法。第 11 章和第 15 章论述了利用网络嗅探器减少入侵的途径。

诱骗 一个用户伪装成另一个用户，一个主机伪装成另一个主机，一个 IP 地址伪装成另一个 IP 地址[②]，一个域伪装成另一个域或地址，所有这些都是诱骗的例子。1.5 节“深入阅读资料”援引的“Hacker Proof”和“Maximum Security”书中对这些入侵方式及防御措施都有详细论述。本书的第 16 章也探讨了各种防御入侵的方法。

TCP/IP 入侵 利用 TCP 网络连接工作方式的入侵难以预防，也难以发现。第 10，11，16 章论述了许多技术以减少其入侵。请参阅 1.5 节 *Hacker Proof* 一书中有关这方面的详细内容。

捕获会话(Session Hijacking) 用户控制网络会话或连接的一种入侵方式，一个特例是 TCP/IP 非同步入侵。请参阅上面的 TCP/IP 入侵。

拒绝服务 阻止正常使用系统和网络资源的任何活动称拒绝服务(DoS)。一般来说，不能杜绝其入侵，但能使拒绝服务攻击非常困难。第 10 章论述了 xinetd 替代 inetd 的方法来防止特定的网络拒绝服务入侵。

其他漏洞 不同的网络和系统应用程序中有不同的漏洞，有些漏洞论述始终贯穿于本书。获知应用程序漏洞的最好方法是即时刷新内容(附录 A)。1.5 节“深入阅读资料”中有其论述。

1.3.2 社会范畴

任何安全策略(参见第 2 章)的最薄弱环节是授权使用计算环境的人。突破最薄弱环节而入侵计算机环境的人从事的活动称其为“社会工程”。在所有的安全环节中，这是最难防的一种行为。1.5.3 节“网址”中有一些普通的社会工程入侵和安全参阅资料。

Shoulder Surfing(窥视) 顾名思义，是捕获敏感信息的过程。例如：偷看别人的口令。

控制 是获得敏感信息的另一种方法。例如，伪装成系统管理员或组织的高级官员从粗心大意的组织人员内部获得敏感信息。

1.3.3 物理范畴

一旦物理安全受到入侵，那么一切都完了。这意味着如果未授权的人获得访问某部分的计算环境，那么任何一种安全解决方案都无济于事。本书将不论述这个主题。1.5.3 节“网址”援引的国际信息系统安全认证协会[(ISC)²]主页中对社会工程安全问题有很好的论述。

访问系统 一旦获得物理访问计算机，那么就可以以单用户模式引导系统从而控制系

② 如果恶意者这样做的话,就是诱骗.可以参看第 16 章的“伪装”。

统。因此应严格禁止物理访问最重要的系统。

联网问题 以电子介质实现联网，例如 10/100Base-T，射频(RF)通信，微波技术以及卫星通信。使用分接(tapping)技术[③]就可截获以上的通信方式。使用光纤介质可极大地防止问题的产生。1.5.3 节“网址”的[(ISC)²]页中有详细论述。

其他物理访问问题 从失火到抢劫等自然灾难都是获得未授权物理访问的例子，1.5.3 节“网址”的[(ISC)²]主页中有详细论述。

1.4 小结

本章概述了与计算机和网络有关的各种漏洞和入侵行为，然而，这并不是本书的要旨，本书的中心是强调系统安全的重要性。有许多参考资料可供进一步学习。

1.5 深入阅读资料

1.5.1 书籍

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

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

3. Barret, Daniel J., *Bandits on the Information Superhighway*, Sebastopol, California, O'Reilly&Associates, Inc., 1996.

4. Chapman, D.brent, and Elizabeth D.Zwichy, *Building Internet Firewalls*, Sebastopol, California, O'Reilly&Associates, Inc., 1995.

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

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

7. Denning, Dorothy E., *Information Warfare and Security*, New York, New York, Addison-Wesley, 1998.

8. Garfinkel, Simson, and Gene Spafford, *Practical UNIX and Internet Security*, 2ded., Sebastopol, California, O'Reilly&Associates, Inc., 1996.

---

③ Newt Gingrich 发现了这种技术。

9. Garfinkel, Simson, and Gene Spafford, *Web Security & Commerce*, Sebastopol, California, O'Reilly & Associates, Inc., 1997.

10. Hughes, Larry Jr., *Actually Useful Internet Security Techniques*, Indianapolis, Indiana, New Riders Publishing, 1995.

11. Icove, David, Et al., *Computer Crime: A Crimefighter's Handbook*, Sebastopol, California, O'Reilly&Associates, Inc., 1995.

12. Klander, Lars, *Hacker Proof: The Ultimate Guide to Network Security*, Las Vegas, Nevada, Jamsa Press, 1997.

13. Kyas, Othmar, *Internet Security Risk Analysis, Strategies and Firewalls*, London, England, International Thomson Computer Press, 1997.

14. Pabrai, Uday O., and Vijay K.Gurbani, *Internet and TCP/IP Network Security Securing Protocols and Applications*, New York, New York, McGraw-Hill, 1996.

15. Siyan, karanjit, Ph.D., and Chris Hare, *Internet Firewalls and Network Security*, Indianapolis, Indiana, New Riders Publishing, 1995.

1.5.2 有趣的黑客故事

此参考资料不是有关技术指南，而是有关著名的入侵故事。

1. Dreyfus, Suelette, *Underground Tales of Hacking, Madness, and Obsession on the Electronic Frontier*, Kew, Australia, Mandarin, 1997.

2. Littman, Jonathan, *The Watchman*, Boston, Massachusetts, Little, Brown and Company, 1997.

3. Shimomura, Tsutomu, with John Markoff, *Takedown*, New York, New York, Hyperion, 1996.

4. Stoll, Cliff, *The Cuckoo's Egg*, New York, New York, Pocket Books, 1990.

1.5.3 网址

有关域名服务(DNS)，内网新闻(INN)和动态主机配置协议(DHCP)的信息，可查看互联网软件协会(ISC)主页：

```
http://www.isc.org
```

sendmail(邮件传输代理)的主页上有许多 sendmail 漏洞的信息。

```
http://www.sendmail.org
```

有关一般安全信息，链接和参考资料可参见信息系统安全协会网站，

http://www.issa-intl.org

(ISC)^2 公司是安全领域的专业认证机构，该网站有技术，物理，人事以及其他领域的安全，其主页为：

http://www.ISC2.org

搜集安全工具和资源的优秀网站当推计算机操作，审计和安全技术(COAST)网站主页：

http://www.cs.purdue.edu/coast/

其他优秀的网站为：

http://www.fish.com/security/
ftp://ftp.porcupine.org/pub/security/index.html

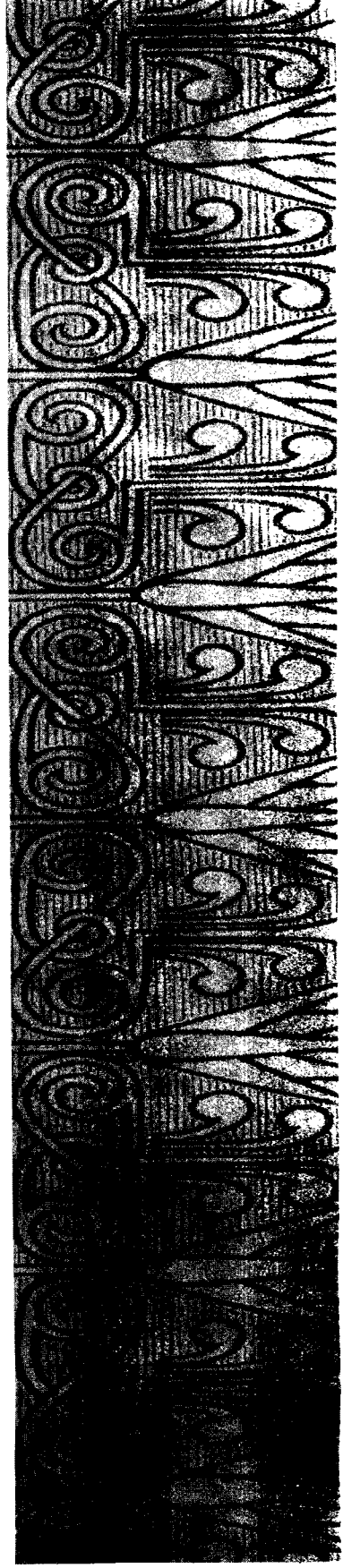
1.5.4 暴露漏洞的资源

下列网站公布了各种漏洞的详细资料以及利用漏洞进行入侵的编码例子。列出下列网址的目的是了解黑客的动向。

http://www.insecure.org/
http://www.10pht.com/
http://www.rootshell.com/
http://www.security-focus.com/

还有未公开的网址列表，请参见：

http://www.cs.purdue.edu/coast/hotlist/ ■



第 2 章

安全策略

从系统和网络管理员的角度来看，安全问题是一个与其无关的字眼。因为，系统和网络管理员的职责并不是简单地区分黑客或警察，而是保持系统正常工作，应用程序正常运行，维护网络服务，令用户满意。但随着计算机技术的日益发展，在越来越大的程度上，系统和网络管理员的职责不得不与安全问题紧密相联。

中央处理器(CPUs)的处理速度越来越快，价格也更加便宜。随机访问内存(RAM)的空间也越来越大，互联网也日益普及，此外，上网的速度也比从前加快，在许多地区实现了aDSL[①]和电缆连网。人们不再局限于速度为 56K 的调制解调器，随着使用计算机与上网人数的不断增加，从事电子商务与服务活动也日益频繁。在线商店、银行以及政府服务只是代表了其中一部分的活动。这些服务的日益扩大反映了更大的生产潜力与破坏潜力。

新一代人的计算机知识水平日益提高，年龄也日益缩小。16 岁左右的年龄段的人可能已是一个很好的编程人员，甚至可能是一个高水平的计算机天才。

正如第 1 章所述，入侵系统并不需要编程技能，要求具备的是访问互联网，特别是访问提供入侵软件及其编辑安装基础知识的互联网网站(第 1 章中列出了一些网站)。因此，计算机黑客人数不断上升。

人们不仅仅关注互联网上的恶作剧，每年，计算机安全协会(CSI)与联邦调查局(FBI)联合进行计算机犯罪与安全调查。1999 年调查报告显示，31%的受访者经历过外部入侵，97%的受访者称内部人员滥用访问系统职权[②]，86%的受访者称，入侵的极大可能性来自于牢骚满腹的员工，还有 53%的受访者称本国的竞争者也具有极大的入侵可能性。上述统计表明，必须重视内外部的未授权访问，必须防备可信与不可信的用户。

随着公共互联网访问人数的不断增加，访问速度加快，入侵工具的实用性，内部人员滥用访问职权等，难怪，CSI/FBI 调查报告显示 1999 年入侵次数比前几年都有所增加，表明这一趋势还会增加。

为了突出此问题，依赖于计算机技术进行电子商务的公司的当务之急是制定保护其系统资源及数据的计划，该项计划通常是安全策略的一部分，安全策略是制定公司资产与数据的配置，维护和使用规则的文件。

本章并没有详细研究安全策略的发展及其前提要求(例如 2.1.2 节“风险分析”部分的风险分析，此主题的详细内容参见 2.5 节“深入阅读资料”)。只是提供了与计算机资源相关主题的一般看法，也是来自于安全策略的经验之谈。现在开始论述计算机与网络安全。

① 非对称数字用户线,提供慢速上联(例如，33-56Kbps)与高速下联(例如，3-6Mbps)。

② 有关完整的情况,参见 http://www.gocsi.com/。

2.1 计算机与网络安全定义

对安全的一种定义，即保护其自身的一种手段。因此，计算机与网络安全也可简单地定义为保护计算机与网络的一种手段。此定义带来了这样的问题：保护资源应防止什么或对付谁，何时有必要？此问题并不是一个简单的问题，依赖于各种因素。因此我们来列举各种计算环境。

2.1.1 计算环境因素

计算环境指计算机、网络及其相互作用，计算环境功能要求按其特点分为：

- 可靠性。
- 完整性。
- 保密性。

计算环境的可靠性是指其始终运行在其配置的方式中。但有许多因素导致了可靠性系统的降低。例如，非确定的停止工作(由于硬件问题，停电等)，偶然的人为因素(意外的重新引导系统或路由器等)，软件错误，拒绝服务。

计算环境的完整性是指该环境数据的正确性，是应用数据和配置数据的结合(口令文件，路由表，域名服务信息等)，由于其他资源和活动-软件错误，偶然引入错误，故意修改数据等原因破坏了计算机的完整性。

保密性是指授权人员使用计算机资源，特别是其数据。偶然的错误配置软件或故意入侵计算环境都可破坏保密性。

因此，可进一步定义计算机和网络安全为保护计算环境的可靠性，完整性和保密性。此定义及可靠性，完整性和保密性的分类提供了分析安全策略整体信息的一种手段。

2.1.2 风险分析

特别是与计算资源有关的风险分析是指估算衰减的或受侵害的计算环境三种因素(可靠性、完整性、保密性)之一或以上的财政成本的过程，其与防御措施财政成本成对比，常指排除衰减或入侵因素的反措施，风险分析的两个重要组成部分是漏洞评估和危险评估。

漏洞评估或漏洞分析是识别消极影响计算环境可靠性，完整性和/或保密性的存在因素。危险评估或危险分析是识别何人企图影响计算环境可靠性，完整性和/或保密性的过程。以上评估必须考虑计算资源的价值及其受攻击的可能性。例如，包含专有信息的数据库服务器就很有价值，比没有专有信息且不能访问公司内部网络的客户工作站易受攻击。

以上分析结果是风险分析的第一步即：估算衰减或受侵害计算环境有关的费用以及发生损失的可能性。根据第一步的风险分析，并依据潜在的损失费用与实施降低风险费用相对

比，采取相应的对策。例如，假如以上提到的数据库服务器漏洞与客户工作站漏洞是一样的，但对付数据库服务器漏洞的措施却很广泛，并需要行政干预和公司开支。但对付客户工作站漏洞措施却不需要诸多干预或巨大开支。

全面的风险分析需要付出巨大的努力，甚至一个小公司的风险分析也要花数月才能完成。分析结果为安全策略提供了基础，因此极具价值性。

2.1.3 安全策略

包含风险分析结果的安全策略提供了管理计算环境的过程。特别是，提供了系统管理员计算环境的操作原则，例如，管理用户帐号原则、安装系统程序原则、系统管理员间的通信程序原则、使用安全工具原则、处理未授权访问的程序原则及识别重要系统以及极重要的改变安全策略的规则。

正确使用安全策略会产生一个连续的、可预测性的环境，更容易发现入侵和未授权访问的反常现象。

正确评估安全策略的价值，是确保计算环境的最关键因素。当然，正确使用和实施安全策略才能确保其真实性。2.5 节“深入阅读资料”列出了许多有价值的资源。

注释

可接受使用策略(AUP)是详细论述组织资产使用权的安全策略的派生词。

2.2 计算机与网络安全

本书详述了确保系统与网络安全的各种开放有效的工具，但在缺乏周密考虑的前提下，使用此工具通常会降低其有效性。因此强烈建议，在缺乏正式安全策略时，制定的计算资源安全计划应是整个安全计划的一部分。2.5 节“深入阅读资料”中提供了更详细的资源。

以下经验之谈是贯穿于本书的指导方针，提供了论述与实施各种安全工具的基础，并提供与计算环境有关的实用哲理。如果某组织制定了安全策略，为了与该组织的安全策略相一致，应对这些经验作相应的修改。

漏洞是不可避免的！完全保护安全系统的方法是没有的，如果启动计算机并与网络相连时，无论采取何种安全措施，该计算机都会有漏洞，并最终导致网络上的其他系统产生漏洞。假如不能识别所有的漏洞与入侵威胁，那么就必须提高警惕并努力坚持确保安全环境。

人是最脆弱的环节！如果公司的员工有权访问内部计算资源的话，那么员工掌握的信息也许对希望入侵该计算环境的人来说，是极具价值的。下面讲述了一些简单的入侵例子。

- 写出难以记忆的口令。
- 对话中，无意泄露了有价值的计算环境信息。