SAMS

Linux

系统安全基础

[美] Aron Hsiao 著
史兴华 译

人民邮电出版社
www.pptph.com.cn

Linux 系统安全基础

[美] Aron Hsiao 著
史兴华 译

人 民 邮 电 出 版 社

图书在版编目(CIP)数据

Linux 系统安全基础/（美）海赛（Hsiao，A.）著；史兴华译. —北京：人民邮电出版社，2002.2
ISBN 7-115-09965-0

I. L… II. ①海…②史… 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 090606 号

版权声明

Linux 系统安全基础

◆ 著 [美] Aron Hsiao
译 史兴华
责任编辑 李 际

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@pptph.com.cn
网址 http://www. pptph.com.cn
读者热线 010-67180876
北京汉魂图文设计有限公司制作
北京朝阳展望印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092 1/16
印张：18.75
字数：437 千字 2002 年 2 月第 1 版
印数：1-4 000 册 2002 年 2 月北京第 1 次印刷

著作权合同登记 图字：01 - 2001 - 0782 号
ISBN 7-115-09965-0/TP • 2679

定价：34.00 元

本书如有印装质量问题，请与本社联系 电话：(010)67129223

内 容 提 要

本书讨论了有关 Linux 系统安全的基本知识，全书共分五大部分、24 章，内容包括：Linux 安装、系统安全、网络安全、数据加密、入侵检测和恢复等。通过学习全部 24 章课程，你可以逐步构建并且运行一个安全的 Linux 网络。

本书内容全面，分析问题详尽、透彻，讲解深入浅出，适合各个层次的 Linux 用户学习和参考。

前　言

在计算机世界中，安全（security）是一个陌生的话题。这是因为，我们所了解的计算机世界在很大程度上已经成为网络功能的技术集合，而且，我们关于网络应该是什么样子的概念与良好的安全应该是什么样子的概念从根本上说是矛盾的。网络的设计明确允许检索数据以及允许无关的计算机和系统之间建立连接。另一方面，安全的任务则主要是禁止检索数据或禁止一台计算机与其他计算机建立连接。这样，很显然，在保护系统或网络安全的过程中，保持前后连贯性和平衡是非常重要的。在你自己的计算机环境中必须具有良好的安全性能，以便为你和你的用户在允许和禁用之间提供一种可接受的平衡。

由于这种矛盾的基于设备场景的本质是计算机安全（computer security）和网络安全（network security）所固有的，也由于对那些想要深入学习的人来说，安全性是一个无穷尽的、越来越艰深的主题，因此，在安全性方面，没有一本书会是安全的终极指南，也没有一本书能够被所有用户或者系统管理员一直用来确保其每个系统的安全。

为什么安全性这么重要呢？

当大型 Internet 服务器里满是用户的信用卡号码，或者大型政府服务器里满是核机密时，显而易见，信息必须受到保护，一些系统之间的连接或是数据检索应当被禁止。这种类型的风险很容易被看到：一方面会发生涉及千千万万人的金融风险，另一方面会危及国家甚至全球的安全。但是，对那些接入互联网只是为了浏览 Web 站点的拨号上网用户怎么办呢？那些经营并不重要的小型 Web 站点、尚不足以成为国际恐怖主义分子或有组织犯罪目标的小型商业用户怎么办呢？

不幸的是，Internet 和现实世界一样，并不总是一个友善的地方。总有一些低级趣味的人想要获取你服务器里的信用卡号码。更可怕的是，数以千计的 script kiddies（脚本小孩）漫游在 Internet 上却根本没有任何动机——他们热衷于侵入计算机系统并清除数据，仅仅是因为好玩。通常他们并不是本领高强的黑客，只是利用从安全类 Web 站点上下载的攻击工具（exploit，用来侵入他人计算机的工具）。

事实上，这两种类型的安全威胁——低级趣味的犯罪分子和不留痕迹的脚本小孩，更喜欢侵入安装在家里和小型商务办公室的计算机系统。为什么呢？因为在大多数时间里，这些系统最缺乏保护。想一想，你采取过什么措施来保护家里的计算机免遭外界的攻击吗？在家用计算机里的数据也许没有什么特别的价值，但是，当你离开已接入 Internet 的计算机去冲一杯咖啡，5 分钟后回来时，发现机器硬盘里的数据已经丢失而且不可恢复了；当你所有的信件、收入支出记录，甚至你的 IE 收藏夹都已丢失，你会做何反应呢？

对于小公司而言，威胁更是显而易见的。如果经营 Web 站点是你的主要收入来源，你当

然不想它被毁掉。更重要的是，所有那些记录——你的生意往来账簿——都会丢失，而这都是你用血汗和泪水苦心经营多年才得来的。

在当今世界，网络安全对每一个 Internet 用户和每一个网络公司来说都是非常重要的。

我正在使用 Linux 系统，怎样才能使它更安全呢？

下面是一些关于一般的家庭或小型公司 Linux 用户的重要特征。一般的 Linux 用户：

- 经常接入 Internet，或者经营一个小型 Web 站点、FTP 服务器或 E-mail 服务器；
- 在标准的 PC 兼容硬件上运行 Linux；
- 安装了商用 Linux 发行版本，可能是 Red Hat Linux；
- 除了版本发行商配置的措施之外，没有采取任何安全措施；
- 很少或从不检查系统日志。

如果你也是这样，那你就要遇到麻烦了，或者可能已经深陷麻烦之中。事实是，大多数 Linux 发行版本从根本上讲是处于不安全状态——基本上允许任何人访问 Linux 能够处理的所有服务。为什么呢？因为 Linux 源自 UNIX 操作系统，并且大多数发行销售商仍然认为是胜任的系统管理员执行所有的 Linux 安装，因而能够在它联机前采取必要措施以保证系统安全。

不幸的是，情况并非总是如此。如果你觉得上述多数特征与你现在的情况相符，你应该立即清楚地意识到：你需要使自己的系统更安全。

这正是本书的切入点。

通过采取一些相对简单的措施，并对你的系统处理各种类型数据和连接请求的方式进行一些修改，就能够使你的 Linux 系统或 Linux 网络比现在安全得多。

我可以使系统足够安全吗？怎样才算得上足够安全呢？

一些经验丰富的 Linux 用户，特别是系统管理员，喜欢说系统永远不可能达到“足够安全”状态，在安全问题上不敢有丝毫松懈。这些人通过他们在对安全性有大量需求的大型组织中的切身经历来说明这一点。对那些既非计算机专业人士又请不起专家的用户来说，一周 7 天、一天 24 小时地盯着安全问题是不现实的。换言之，在某些方面对安全性的关注可以被认为是“足够”的。

当然，对家庭和小型商业 Linux 用户在安全性帮助方面的需要也有好消息。尽管你的系统可能是那些低级趣味的骗子或者脚本小孩入侵的理想选择，但它可能还不会大到足以成为一个黑客专家或黑客组织实施系统攻击的目标。因此，对你而言，足够的安全是能够定义的，或者至少是可以设想的。

通过采取被安全专家认为是良好的安全策略基础的一些简单措施，时刻保持警惕，了解你自己的系统和你自己的 Linux 设置，你可以预防大多数攻击并关闭大多数漏洞。简而言之，你可以保护好你的数据和机密，让你的内心平静一些。本书将涉及到的一些你必须采取的措施，归纳如下：

- 确信你的物理环境没有安全隐患；
- 谨慎安装 Linux 以及你能找到的所有更新，以安全为出发点；
- 对所有的系统设置都加上口令，并选择那些不易猜到的口令；
- 指示你的文件系统不要向那些不应该获得它们的人泄露任何秘密；

- 关闭不需要的网络服务；
- 对于你确实需要的网络服务，要严格审核连接用户及其相关数据；
- 如果你有网络的话，可利用防火墙或包过滤加以保护；
- 加密所有通过网络传输的敏感数据；如果需要，也要加密本地存储的敏感数据；
- 对每件事都进行日志记录，并懂得如何监控日志，定期检查漏洞；
- 维护好备份，在遭到攻击或侵入时知道如何恢复备份。

这些是计算机和网络安全的基础。有了它们，绝大多数来自脚本小孩和业余黑客的攻击就会当场失败。对于大多数家用和小型商用 Linux 用户来说，这一系列措施就代表着足够的安全性。

本书的结构

全书一共 24 章，分成相互连贯的几部分。一些用户可以跳过其中几章，例如，使用单个 PC 机的家庭用户可以略过 Kerberos 验证这一章。但是，不论你是如何使用你的系统，作为一个 Linux 和 Internet 用户来讲，在本书包括五个部分，每一部分都包含了一些对你有用的内容。

第一部分——“适合所有任务的基本安全”讨论了一些与特殊的网络服务或特定的任务类型的安全需要不相关的安全基础。这一部分包括安装和配置 Linux 系统时最简单，也是最容易被忽略的内容，将涉及到有关物理安全（硬件和位置）、操作系统——独立的安全问题、Linux 安装、引导、账号、口令、文件权限和 TCP wrappers（网络安全的最基本形式）等内容。

第二部分——“网络安全”讨论了在互联网环境中使用 Linux 的有关问题，特别是将 Linux 用作各种类型数据服务的小型服务器的相关问题。这一部分将涉及到防火墙和包过滤、Kerberos 认证、与单个网络服务相关的安全性，包括 Web 服务、X11R6 显示和数据流的安全性等。

第三部分——“数据加密”在内容上更加深入，将与你探讨有关加密敏感数据的过程。首先，你将学习利用 SSH 安全 shell 和它的隧道功能，加密你的计算机系统中输入、输出的各种数据流。这一部分还包括提供加密的（安全的）Web 会话、使用两种不同工具加密你的本地文件系统、使用 PGP（Pretty Good Privacy）和 GPG 加密你的 E-mail 等内容。

第四部分——“入侵检测、审核和恢复”将帮助你增强在前几部分中对你的系统所做的防御措施。你将学习审核你的系统中仍然存在的安全隐患、监控活动系统受到的正在进行的攻击或者可疑活动、理解攻击可能造成的系统漏洞以及从不幸的攻击中恢复等内容。

第五部分——“附录”包含一些快速参考数据，用以帮助你处理 Linux 系统和 Linux 网络中的安全问题。附录 D——“快速安全清单”包含一个简化的分类清单，对于家庭或小型商业用户是非常重要的。在完成每一章内容以后，为了能够清楚地看到你的 Linux 环境变得更加安全的过程，你可以参考一下这个清单。

言归正传。现在我们开始学习如何保护你的数据。

目　录

第一部分　适合所有任务的基本安全