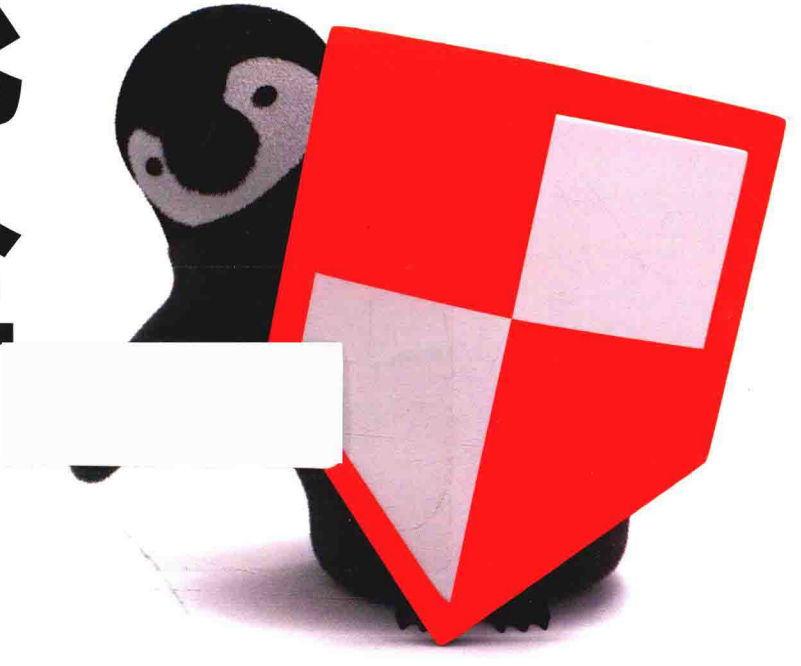
HZ BOOKS
华章IT

Linux/Unix
技术丛书

Linux

Practical Linux Security Cookbook

系统安全



[印] 达金德尔·卡尔西
(Tajinder Kalsi) 著

刘海燕 等译

机械工业出版社
China Machine Press

Linux 系统安全

Practical Linux Security Cookbook

[印] 达金德尔·卡尔西 (Tajinder Kalsi) 著

刘海燕 等译

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

Linux 系统安全 /（印）达金德尔·卡尔西（Tajinder Kalsi）著；刘海燕等译 . —北京：机械工业出版社，2017.12
（Linux/Unix 技术丛书）
书名原文：Practical Linux Security Cookbook

ISBN 978-7-111-58631-9

I.L… II.①达… ②刘… III. Linux 操作系统 - 安全技术 IV. TP316.85

中国版本图书馆 CIP 数据核字（2017）第 298877 号

Linux 系统安全

出版发行：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：缪 杰
责任校对：殷 虹
印 刷：北京兆成印刷有限公司
版 次：2018 年 1 月第 1 版第 1 次印刷
开 本：186mm × 240mm 1/16
印 张：13.75
书 号：ISBN 978-7-111-58631-9
定 价：59.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88379426 88361066
投稿热线：（010）88379604
购书热线：（010）68326294 88379649 68995259
读者信箱：hzit@hzbook.com

The Translator's Words 译 者 序

Linux 是个开源的操作系统，以模块化、通用性、可靠性、可扩展性著称，拥有强大的社区支持。其开放、共享的精神持续吸引着众多 IT 精英投入 Linux 操作系统及相关应用的开发之中，适应各种需求的平台和工具不断推出。在应用方面，越来越多的服务器和网络应用选择 Linux 作为运行平台。据国际 TOP500 组织公布，在全球超级计算机 500 强中，Linux 占据操作系统的 94.2%。

Linux 的另一个巨大优势就是它的安全性，它被认为是当今世界最安全的操作系统。Linux 的安全性得益于它的如下特点：卓越的补丁管理工具，可以在自动更新系统的同时升级系统中所有的软件；较为健壮的默认设置和权限管理，能将攻击带来的危害限定在一定范围内；模块化设计，使得用户可以选择安装或删除任何一个系统组件；系统中默认整合的 SELinux 等安全机制，能够为系统提供保护；开放源代码构架，能更容易、更快速地发现和修复系统的安全问题等。

然而，Linux 毕竟是一个通用操作系统，为了满足更广泛的用户需求，Linux 操作系统以及应用软件都提供了多种配置参数，默认的设置安全性还不够。管理员应该根据自己的安全需求，制定相应的安全策略，运用各种命令和工具进行合理的配置，并对系统的运行进行监控。因此，Linux 的安全性最终取决于管理员实施的管理措施，管理员有责任以使其变得更安全的方式来配置机器。

本书以提高 Linux 系统主机的安全性为目标，从内核配置、文件系统安全、安全认证、网络安全以及 Linux 上的安全工具等多个方面，展开实践指导。书中没有深奥的理论或者高级的设计。针对每个主题，结合常见任务，用简洁的步骤描述、直观的屏幕截图和详细的原理解释，循序渐进地介绍提高 Linux 系统安全性的方法。书中内容读起来容易理解，操作起来简单易行，非常适合于自学。本书是 Linux 系统用户以及网络管理人员学习加固

自己的 Linux 桌面系统和服务器系统的不二选择。

Linux 的安全是个庞大的主题，尽管本书作者对书的主题及内容进行了取舍，但涉及的主题仍十分广泛。作为本书的翻译人员，我们的原则是保证译文能反映作者的真实意图，同时力求以通俗的语言进行有效表达；对于涉及的命令、软件工具、专业术语等，我们参考国内同行在 Linux 系统及信息安全领域的习惯用法进行相应的翻译；对于一些普通用户可能不熟悉的关键术语或命令，我们增加了适当的译者注，希望这些译者注能在你遇到困难时助你茅塞顿开。

本书是一本操作性、实战类书籍。实践出真知，读者在学习过程中一定要自己实际动手来操作，才能体会每个步骤的细节要求，理解每种方法的作用。书中的每种方法按照准备工作、操作指南和原理解析三部分进行说明。其中，准备工作部分是应用方法的前提，而原理解析部分是对方法进一步的解释，操作指南部分以文字说明、命令展示以及屏幕截图的方式说明方法的详细步骤。读者在应用某个方法时，应设法满足方法的前提条件，遵循步骤的要求，其中的一些参数可能需要根据实际情况进行调整。此外，根据我们的使用经验，书中部分方法的细节操作可能特定于某个版本，而由于 Linux 系统及软件的版本发展非常快，读者使用的软件版本可能不同，这时读者可以参照书中的步骤，根据自己的实际版本进行对应性调整。我们相信，只要你遵循了操作步骤和要求，就一定能得到预期的结果。

本书的第 1 和 2 章由刘海燕翻译，第 3 和 4 章由常成翻译，第 5 和 6 章由李皓翻译，第 7 和 8 章由王璇翻译，第 9 和 10 章由武卉明翻译，其余部分均由刘海燕翻译，全书由刘海燕统稿和修改。因水平和时间所限，译文在理解和表述方面难免存在不当之处，请读者批评指正。

Preface 前　言

在建立 Linux 系统时，安全性在各个阶段都被认为是重要部分。通晓 Linux 的基本知识对在机器上实现良好的安全策略至关重要。

Linux 系统的安全性不是天生就完美的，因而，管理员有责任以使其变得更安全的方式来配置它。

本书是帮助管理员配置更安全的机器的实用指南。

如果你想了解 Linux 的内核配置、文件系统安全、安全认证、网络安全以及 Linux 上的各种安全工具，那么本书就能满足你的需求。

Linux 安全是一个庞大的主题，仅用一本书不足以涵盖所有的内容。不过，本书仍将提供很多方法来帮助你加固机器。

本书主要内容

第 1 章　涵盖 Linux 有关的各种漏洞及利用，还讨论了应对这些漏洞的安全方法。内容包括制定安全策略并进行安全控制以用于口令保护和服务器安全，对 Linux 系统进行脆弱性评估。本章还将讨论 sudo 访问的配置方法。

第 2 章　重点介绍 Linux 内核的配置和构建过程以及它的测试。内容包括构建内核的要求、配置内核、安装内核、定制内核以及内核的调试等。本章还将讨论如何使用 Netconsole 配置一个控制台。

第 3 章　着眼于 Linux 系统的文件结构和访问权限。内容包括查看文件和目录的详细信息、使用 chmod 处理文件和文件访问权限、实现访问控制列表等。本章还将向读者介绍 LDAP 的配置。

第 4 章 探讨安全的本地系统用户认证。内容包括用户认证的日志记录、限制用户的登录能力、监视用户行为、定义授权控制以及如何使用 PAM。

第 5 章 讨论 Linux 系统的远程用户认证。内容包括使用 SSH 远程访问服务器、禁用和启用 root 用户登录、限制使用 SSH 时的远程访问、通过 SSH 远程复制文件以及设置 Kerberos。

第 6 章 讨论关于网络攻击和网络安全的问题。内容包括管理 TCP/IP 网络、使用 iptables 配置防火墙、阻止伪造地址和不需要的入站流量等。本章还将介绍 TCP Wrapper 的配置和使用。

第 7 章 介绍可用于 Linux 系统的各种安全工具或软件。涉及的工具包括 sXid、PortSentry、Squid 代理服务器、OpenSSL 服务器、Tripwire 和 Shorewall。

第 8 章 介绍与安全和渗透测试有关的几个著名的 Linux/UNIX 发行版本，包括 Kali Linux、pfSense、DEFT、NST 以及 Helix。

第 9 章 探讨著名的 bash shell 漏洞——Shellshock。本章将介绍什么是 Shellshock 漏洞以及该漏洞可能引起的安全问题，同时告诉读者如何使用 Linux 补丁管理系统来加固自己的机器，以及在 Linux 系统中补丁是如何应用的。

第 10 章 介绍 Linux 的本地系统及网络的监控问题。内容包括使用 Logcheck 监控日志、使用 Nmap 监控网络、使用 Glances 监控系统以及使用 MultiTail 监控日志。本章还将讨论一些其他的工具，包括 Whowatch、stat、lsof、strace 和 Lynis 等。

学习本书的要求

为了充分发挥本书的作用，读者应该对 Linux 的文件系统和管理有基本的了解，应该知道 Linux 的基本命令，如果有一些信息安全的知识则更佳。

本书包括基于 Linux 系统内置工具以及其他一些开源工具进行安全管理的例子。对每一种方法，如果所用的工具在 Linux 上还没有安装，那么请读者务必要安装它们。

本书的目标读者

本书面向所有已经了解 Linux 文件系统及管理的 Linux 用户。读者应该熟悉 Linux 的基本命令，理解信息安全知识以及 Linux 系统的安全风险也有助于理解书中的方法。

然而，即使你对信息安全不熟悉，也能够很容易地遵照执行和理解书中讨论的方法。

因为本书遵循了实用性原则，按照步骤进行操作非常容易。

内容分节

本书中，你会发现一些标题出现的频率很高，如准备工作、操作指南、原理解析、拓展学习、延伸阅读等。

为了更清楚地说明如何实现一种方法，我们使用了如下几个标题。

准备工作

该部分告诉读者本方法的目标，描述如何设置软件以及本方法要求哪些预先设置。

操作指南

该部分包括实现本方法所需的步骤。

原理解析

该部分通常包括对操作指南部分所发生情况的详细解释。

拓展学习

该部分是为使读者对本方法有更多了解而提供的附加信息。

延伸阅读

该部分为其他有用信息提供帮助链接。

下载彩图

我们还为你提供了一个 PDF 文件，里面有书中用到的屏幕截图和图表的彩色图像。彩色的图像将帮助你更好地理解输出中的变化。

你可以从下述地址下载此文件：http://www.packtpub.com/sites/default/files/downloads/PracticalLinuxSecurityCookbook_ColoredImages.pdf。

目　录 Contents

第 1 章 Chapter 1

Linux 的安全问题

本章将讨论如下主题：

- Linux 的安全策略
- 配置口令保护
- 配置服务器安全
- 使用校验和检测安装介质的完整性
- 使用 LUKS 加密磁盘
- 配置 sudo 访问
- 使用 Nmap 扫描主机
- 获取脆弱 Linux 系统的 root 权限

1.1 引言

一个 Linux 系统的安全性取决于管理员对它的配置。在安装完 Linux 系统并删除所有不必要的软件包之后，我们就可以开始处理 Linux 上软件及服务的安全问题了。

1.2 Linux 的安全策略

安全策略是指为保证一个组织的计算机网络安全而必须遵循的规则及实践。它还定义了组织如何管理、保护以及发布敏感数据。

那么，如何制定安全策略呢?

在创建安全策略时，我们应该确保安全策略简单易用。策略的目标应该是保护数据，同时维护用户隐私的完好。

安全策略的制定应围绕如下几点：

- 对系统的访问能力
- 系统上安装软件的权限
- 数据的访问权限
- 从故障中恢复的方法

在设计安全策略时，应保证一个用户仅能使用那些已经授权的服务，任何不允许的操作都应该在策略中进行限制。

1.3 配置口令保护

在任何系统中，口令对安全性都起着非常重要的作用。不好的口令可能会导致组织的资源受到损害。为此，组织中的每个人，无论是普通用户还是管理员，都应该遵守口令保护策略。

操作指南

下面给出一些在选择口令或加固口令时必须遵循的规则：

口令的创建策略应遵循如下规则：

- 一个用户在组织中的所有账号不能使用相同的口令。
- 所有与访问相关的口令都应该互不相同。
- 当同一个用户既有系统级账号又有普通账号时，系统级账号的口令一定与其他账号的口令不同。

口令的保护策略应遵循如下规则：

- 口令应该被看作敏感和机密的信息，因此不能与任何人分享。
- 不应该通过任何电子通信工具（如电子邮件）共享口令。
- 永远不要在手机上或者调查问卷中透露口令。
- 不要使用能向攻击者提供线索的口令提示。
- 不要与任何人分享公司的口令，包括行政人员、管理者、同事，甚至家庭成员。
- 不要将口令以书面形式存储在办公室的任何地方。如果将口令存储在移动设备上，

那么一定要进行加密。

- ❑ 不要使用应用程序的口令记忆功能。
- ❑ 如果怀疑口令可能被泄露，那么要尽早上报安全事件并更改口令。

口令的更改策略应遵循以下规则：

- ❑ 所有用户和管理员必须定期更改口令，至少每季度修改一次。
- ❑ 组织的安全审计人员必须进行随机检查，检查任何用户的口令是否能够被猜出或者被破解。

原理解析

在创建或更改口令时遵循上述规则，可以确保口令不那么容易被猜出来或被破解。

1.4　配置服务器安全

Linux 服务器存在恶意攻击的一个主要原因是安全实施不当或者存在漏洞。在配置服务器时，需要正确地执行安全策略，而且，为了正确地配置服务器，需要接管系统的所有权。

操作指南

通用策略如下：

- ❑ 管理一个组织内的所有服务器是专门团队的职责，它还应该负责监视任何形式的违规行为。如果发生了任何违规情况，该团队应该相应地执行或审查安全策略。
- ❑ 在配置内部服务器时，必须登记并确定它们的下列信息：
  - 服务器的位置
  - 操作系统的版本及其硬件配置
  - 正在运行的服务和应用程序
- ❑ 管理系统中的任何信息必须始终保持最新状态。

配置策略如下：

- ❑ 服务器的操作系统应按照信息安全团队认可的指导方针进行配置。
- ❑ 任何不使用的服务和应用程序，如果可能的话都应该被禁用。
- ❑ 对服务器上所有服务和应用程序的访问都应该被监视并记录，而且它们还应该通过访问控制方法进行保护。本书第 3 章将介绍一个这样的示例。
- ❑ 系统应保持更新，任何可用的新安全补丁都应该尽早安装。
- ❑ 尽量避免使用 root 账号。最好使用“最小权限”安全原则，即仅授予执行一项功

能所需要的最小权限。

- 任何特权访问都应该尽可能通过安全信道连接（如 SSH）。
- 服务器的访问应该在受控环境中进行。

监控策略如下：

- 服务器系统中所有与安全相关的操作都必须记录下来，并且按如下方式保存审计报告：
  - 1 个月之内，所有安全相关的日志应在线保留
  - 1 个月之内，每日的备份和每周的备份都应该留存
  - 至少 2 年之内，每月的备份都应留存
- 任何破坏安全的事件都应该报告给信息安全团队，他们将审查日志，并把事件上报给 IT 部门。

下面给出几个安全相关事件的示例：

- 端口扫描有关的攻击
- 未经授权访问特权账号
- 由于主机上出现某特定应用程序而导致的异常事件

原理解析

在对组织拥有的或者组织所运行的内部服务器进行基本配置时，要遵循前面提到的有关策略。有效地执行这些策略，将会减少对敏感信息及私有信息的任何非授权访问。

拓展学习

当谈论 Linux 的安全时，我们还有更多的事情需要去探究。

1.5 安全控制

当我们讨论保护 Linux 机器时，通常总是从一个旨在加固系统的检查清单开始。检查清单能够保证，只要遵循该清单，就可以确认主机是否已经实施了适当的安全控制。

1.6 使用校验和检测安装介质的完整性

当我们下载任何 Linux 发行版的映像文件时，应该检查它的正确性和安全性[⊖]。这可

⊖ 如果安装文件被动了手脚，如被内置了病毒、木马等恶意程序，那么安装的系统本身就不安全。——译者注

以通过对下载后的映像文件计算 MD5 校验和[⊖]，并把它与正确映像文件的校验和进行比对来实现。

校验和可用于检查一个文件的完整性，因为对文件的任何修改都会使 MD5 哈希值发生变化。

一旦下载文件被修改，通过 MD5 哈希值比较就可以检测出来。文件越大，被修改的可能性也越大。因此我们强烈建议对外来的文件（如光盘上的操作系统安装文件等）做 MD5 哈希值比较。

准备工作

通常，大多数 Linux 发行版中都已经安装了 MD5 校验和工具，所以不需要额外安装。

操作指南

1. 首先，打开 Linux 终端，执行命令 ubuntu@ubuntu-desktop:~$ cd Downloads，将当前目录更换到包含下载的 ISO 文件的目录（本示例中，假设下载文件所在的目录为 Downloads）。

注意： Linux 系统是大小写敏感的，因此输入目录名称时一定要拼写正确，例如 Downloads 与 downloads 在 Linux 中是不同的目录。

2. 改变目录到 Downloads 目录之后，输入如下命令：

```
md5sum ubuntu-filename.iso
```

这里的 ubuntu-filename.iso 是下载的映像文件的名称。

3. md5sum 命令将在屏幕上输出指定文件的 MD5 哈希值，如下所示：

```
8044d756b7f00b695ab8dce07dce43e5 ubuntu-filename.iso
```

把上述计算结果与 UbuntuHashes 页面上给出的哈希值进行比较。打开 UbuntuHashes 页面（https://help.ubuntu.com/community/UbuntuHashes），把上述计算的哈希值复制到浏览器的查找框（按 <Ctrl + F > 键可弹出浏览器的查找框）。

原理解析

如果计算出的哈希值与 UbuntuHashes 页面给出的哈希值匹配，那么可以确定下载的

⊖ MD5（Message Digest 5）是一种哈希算法，对任何大小的输入通过运算输出 128 位的哈希值。——译者注

文件没有损坏。如果哈希值不匹配，则可能是下载的文件有问题，也可能是下载服务器有问题。试着再次下载文件，如果问题仍存在，那么建议你将问题报告给服务器的管理人员。

拓展学习

如果你想多学一点知识，那么可以尝试 Ubuntu 上提供的图形用户界面的校验和计算器。

有时，在终端上执行校验和计算确实不太方便。你需要知道下载文件所在的目录以及确切的文件名，要记住确切的命令内容有些困难。为解决这个问题，可以使用一款叫作 GtkHash 的小工具。你可以用如下命令从 http://gtkhash.sourceforge.net/ 下载并安装它：

```
sudo apt-get install gtkhash
```

1.7 使用 LUKS 加密磁盘

在某些企业（如小型公司或政府机关），用户可能需要加固系统以保护私人数据，包括客户的详细资料、重要文件、联系方式等。为此，Linux 提供了大量的加密技术，可用于保护物理设备（如硬盘或可移动介质）上的数据。其中，Linux 统一密钥设置（Linux Unified Key Setup，LUKS）就是这样一个加密技术，它允许对 Linux 的分区进行加密。

LUKS 具有如下功能：

- 可以使用 LUKS 加密整个块设备，非常适合于保护可移动存储介质或笔记本磁盘的数据。
- 一旦被加密，块设备上的内容看起来就像是随机的，所以它对于交换设备的加密非常有用。
- LUKS 使用了现有的设备映射内核子系统。
- 它提供了一个密码加强器，有助于防止针对密码的字典攻击。

准备工作

为完成下述操作，要求在安装 Linux 系统时必须将 /home 目录创建在单独的分区上。

警告：按照如下步骤配置 LUKS 时，将删除加密分区上的所有数据。因此，在开始使用 LUKS 之前，一定要将数据备份到外部资源上。

操作指南

按如下步骤对目录进行手动加密：

1. 转换到运行级别 1。在 shell 提示符或终端上键入以下命令：

```
telinit 1
```

2. 使用如下命令卸载当前的 /home 分区：

```
umount /home
```

3. 如果有其他进程正在控制 /home 目录，那么上述命令会执行失败。这时，可使用如下所示的 fuser 命令查找并杀死这样的进程：

```
fuser -mvk /home
```

4. 执行如下命令检查并确保 /home 分区当前没有被挂载：

```
grep home /proc/mounts
```

5. 现在，在分区中放入一些随机数据：

```
shred -v --iterations=1 /dev/MYDisk/home
```

这里的 MYDisk 是磁盘的设备名。

6. 上述命令可能需要一些时间才能完成，所以要有耐心。时间长短取决于你设备的写入速度。

7. 一旦上述命令执行完毕，则初始化分区：

```
cryptsetup --verbose --verify-passphrase luksFormat /dev/MYDisk/
home
```

8. 打开新创建的加密分区：

```
cryptsetup luksOpen /dev/MYDisk/home
```

9. 检查并确认设备是否存在：

```
ls -l /dev/mapper | grep home
```

10. 现在，创建文件系统：

```
mkfs.ext3 /dev/mapper/home
```

11. 然后，挂载新的文件系统：

```
mount /dev/mapper/home /home
```

12. 确认文件系统仍然是可见的：

```
df -h | grep home
```

13. 在 /etc/crypttab 文件输入如下一行：