LINUX

- 技术全面，囊括 Linux 文件安全的方方面面
- 由浅入深，无论菜鸟高手都可从中获益
- 贴近现实，作者多年实际工作的详细总结

系统文件安全实战全攻略

陶利军　编著

Linux

人民邮电出版社
POSTS & TELECOM PRESS

LINUX

系统文件安全实战全攻略

陶利军　编著

Linux

人民邮电出版社
北京

图书在版编目（CIP）数据

Linux系统文件安全实战全攻略 / 陶利军编著. --
北京 : 人民邮电出版社, 2011.10
ISBN 978-7-115-26124-3

Ⅰ. ①L… Ⅱ. ①陶… Ⅲ. ①Linux操作系统－安全技术 Ⅳ. ①TP316.89

中国版本图书馆CIP数据核字(2011)第151585号

内 容 提 要

本书从保护 Linux 系统文件完整性、Linux 系统下文件病毒的防治、恢复损坏文件等方面，详细介绍了 Linux 系统下与文件安全保护相关的各种软件的应用技巧。本书主要介绍了 Tripwire、AIDE 等软件的工作特性及使用技巧，应用 ClamAV 防治病毒的方法，以及如何使用 ext3grep、extundelete 等软件恢复人为删除的文件。本书实例丰富，讲解透彻，适合 Linux 系统初级管理员及 Linux 系统安全维护人员等阅读。

Linux 系统文件安全实战全攻略

◆ 编　　著　陶利军
责任编辑　汪　振
◆ 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　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京铭成印刷有限公司印刷
◆ 开本：787×1092　1/16
印张：23
字数：563 千字　　2011 年 10 月第 1 版
印数：1－3 000 册　　2011 年 10 月北京第 1 次印刷

ISBN 978-7-115-26124-3

定价：49.00 元

读者服务热线：(010)67132692　印装质量热线：(010)67129223
反盗版热线：(010)67171154

前　言

任何事情存在都有它的道理，Linux 操作系统下的文件也是一样。如果存在着安全，那么也就一定存在着不安全。因此，我们有必要认识什么是安全和不安全。

无论你是简单的办公环境，还是比较繁忙的公司业务，系统安全总是必不可少的，然而性能和安全可能总会成反比，不过如果一味地去追求效率性能而抛弃安全，那么出问题就会成为必然。对于安全，千万不要抱着侥幸心理，安全问题无处不在，可以说它出现有随机性，但是随机的背后却会隐藏着必然性，因此，责任安全无小事，一定要安全在前，生产在后。

本书是我在运维工作中的一点总结，谈不上是什么高深的理论，而且我也觉得没有什么必要去谈理论，实践出真知，因此我们就从实际的部署开始去研究 Linux 系统下文件的安全防范。一定要记住，安全运维无小事，偶然之后隐藏着必然，这是我们安全工作者和运维工作者必须具备的思想。

本书内容

本书共包括了 3 个部分，共 15 章的内容：

上　　篇　文件完整性

中　　篇　Linux 下病毒的防治

下　　篇　恢复认为损坏的文件

上篇　文件完整性

在上篇中，包括了以下 9 章内容，主要介绍的是文件的完整性。

第 1 章　介绍 Tripwire 软件。这一部分是专门为没有接触过 Tripwire 软件的系统管理员，或者是不熟悉完整性评估(integrity assessment)的安全工作者而准备的，如果是有经验的 Tripwire 用户，可以直接跳过本章。

第 2 章　使用 Tripwire。这一章描述的是配置文件和 Tripwire 软件安装后的使用，以及 Tripwire 软件的安装。

第 3 章　Tripwire 命令参考。本章主要介绍了 Tripwire 的命令及其工作模式。

第 4 章　策略参考。这一部分描述的是 Tripwire 策略文件的组成。策略文件包括一系列的规则，以便控制 Tripwire 软件检测系统。对于 UNIX 和 Linux 系统来说，被扫描的系统对象就是文件和目录。

第 5 章　配置文件参考。这一章讲述的是配置文件 tw.cfg，这个文件存储了 Tripwire 软件的配置信息，如用于完整性检测的文件存储位置等。

第 6 章　Tripwire 使用实例。本部分以实验的形式讲述了 tripwire 软件的安装与部署。

第 7 章　认识 AIDE。本章主要介绍 AIDE 的功能、安装要求以及它的基本用法和它的工作

流程图，最后还会介绍其安装后的目录结构。

第 8 章　使用 AIDE。本章主要讲述 AIDE 的使用，并讲述了配置文件和 AIDE 的规则。

第 9 章　使用 ICU。本章讲述 ICU 服务器的原理、构建和使用。

中篇　Linux 下病毒的防治

中篇共包括 5 章内容，主要讲述了 ClamAV 的应用，通过它来保护文件。

第 10 章　Clam AntiVirus。本章主要是对抗病毒软件 Clam AntiVirus 进行讲述，掌握它的安装以及认识 CVD 的格式。

第 11 章　Clamd 服务器。本章主要介绍编译安装 clamav、定制配置文件及与其他服务的结合。

第 12 章　Clamd 与用户文件系统。本章的主要介绍 clamfs 用户文件系统，clamuko 、dazuko 及 dazukofs。

第 13 章　Linux 下的服务与 Clamdav。本章讲述的是运行在 Linux 的各种服务与 clamdav 的结合，以便使用 clamav 对服务进行防护。

第 14 章　监控与管理 clamd。本章中我们首先为 Clamd 建立一个启动管理脚本，这样就可以通过 service 命令来对 clamd 进程进行管理；然后介绍了两个工具，即 clamdmon 和 clamdwatch 工具；最后是 ClamAV 提供的 8 个命令：clamd、clamconf、clamdscan、clamdtop、clamscan、freshclam、sigtool、clamav-config，不同的命令提供了不同的功能。

下篇　恢复人为损坏的文件

下篇主要讨论了如何在 ext3 和 ext4 文件系统下恢复人为删除的文件。

第 15 章　对 ext3 下的文件恢复。任何一个系统管理员，无论是有经验的老手还是没有经验的新手，误删除一个有用的文件是迟早会发生的事，发生了这种事后果你比谁都清楚，因此，在这一章中我们主要研究 ext3 下人为删除文件的恢复。

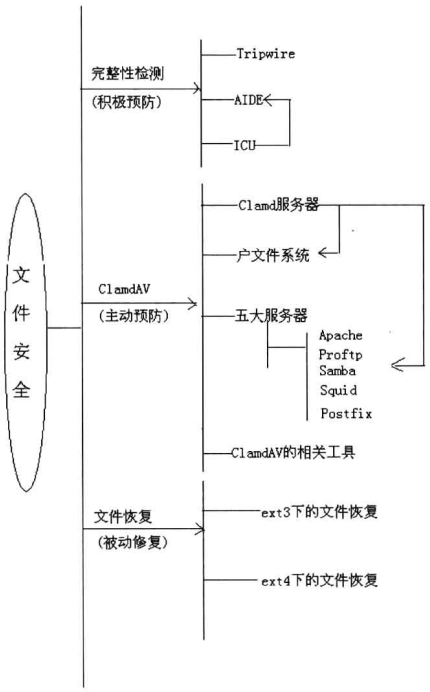
第 16 章　对 ext4 下的文件恢复。由于 ext4 文件系统现在已经被一些 linux 版本使用，因此我们也有必要掌握该文件系统下人为删除文件的恢复，本章正是本着这个出发点而写的。

使用对象

- 广大的 Linux 爱好者
- 具有一定 Linux 基础的系统管理员
- Linux 系统安全管理员
- 讲授 Linux 安全的培训机构

内容导读

本书分为 3 个部分，每一部分都可以单独阅读，它们之间没有必然的联系，然而对于每一部分中的内容，除第三部分外，最好按照章节的顺序阅读，否则会带来很大的障碍。



作者声明

本书的内容是作者在工作中的一个总结，所有技巧在生产环境中都使用过，并非纸上谈兵。但是书中的例子，我尽可能地不使用生产环境中的实际例子，一是怕对读者造成误导，二是不愿意泄露公司的“机密”。

对于文稿的构成，一部分是作者在实际工作中所使用的员工培训的文稿，一部分是在培训中心的文案，还有一部分是作者自己的学习笔记。全书由这三部分融合而成，而非简单的拼凑，之所以强调这些，还是想向读者说明责任安全无小事，要仔细认真地将安全知识运用到生产中去。希望本书能给你带去实际的运用。

由于本人才疏学浅，因此书中难免会有疏漏和不足，如果广大读者如果有什么建议和意见，可以通过邮箱联系作者：linux_file_safe@126.com。

陶利军

2011-10-1

目　录

上篇　文件完整性

第 1 章　Tripwire 软件简介 ……2

1.1　什么是 Tripwire……3
1.2　Tripwire 软件的部署……3
1.3　Tripwire 软件的组成……4
1.3.1　目录结构……4
1.3.2　部分文件的作用……5
1.3.3　非对称加密……6
1.4　Tripwire 软件工作原理……6

第 2 章　Tripwire 的安装与部署 ……8

2.1　Tripwire 软件的编译安装……9
2.1.1　安装环境……9
2.1.2　下载 Tripwire 软件……9
2.1.3　解压压缩包……9
2.1.4　编译安装……9
2.1.5　安装过程……12
2.2　定制 Tripwire 软件……14
2.2.1　修改配置文件……14
2.2.2　测试邮件……15
2.2.3　修改策略文件……15
2.2.4　生成二进制加密签名策略文件……18
2.3　初始化数据库……18
2.4　进行完整性检测……18
2.5　查看完整性检测报告……21
2.6　Tripwire 软件退出代码……23

第 3 章　Tripwire 软件命令参考 24

3.1　tripwire 命令工作模式 25
3.1.1　tripwire 命令的数据库初始化模式 26
3.1.2　tripwire 命令的完整性检测模式 27
3.1.3　tripwire 命令的数据库升级模式 28
3.1.4　tripwire 命令的策略升级模式 30
3.1.5　tripwire 命令的测试模式 31
3.2　twprint 命令 32
3.2.1　twprint 命令的屏幕打印检测报告模式 32
3.2.2　twprint 命令的屏幕打印数据库模式 33
3.3　twadmin 命令 34
3.3.1　twadmin 命令的建立配置文件模式 34
3.3.2　twadmin 命令的打印配置文件模式 35
3.3.3　twadmin 命令的建立策略文件模式 35
3.3.4　twadmin 命令的打印策略文件模式 36
3.3.5　twadmin 命令的移除加密模式 37
3.3.6　twadmin 命令的加密文件模式 37
3.3.7　twadmin 命令的检测加密模式 38
3.3.8　twadmin 命令的创建密钥模式 39
3.4　siggen 命令 39

第 4 章　策略参考 41

4.1　策略文件的组成 42
4.2　规则（Rules） 42
4.2.1　对象名字（Object Names） 43
4.2.2　属性掩码（Property masks） 44
4.3　停止点（Stop Points） 45
4.4　规则属性（Rule attributes） 46
4.4.1　rulename 属性 47
4.4.2　emailto 属性 47
4.4.3　severity 属性 48
4.4.4　recurse 属性 48
4.5　指令 48

4.5.1 指令@@section 49
4.5.2 指令@@ifhost, @@else, @@endif 49
4.5.3 指令@@print, @@error 50
4.5.4 指令@@end 51
4.6 变量（Variables） 51
4.6.1 变量定义 51
4.6.2 变量替换 51

第 5 章 配置文件参考 53

5.1 配置文件（Configuration File） 54
5.1.1 介绍 install.cfg 文件 54
5.1.2 tw.cfg 配置文件格式 56
5.2 配置文件的变量 57
5.2.1 必选变量（Required Variables） 57
5.2.2 可选变量（Optional Variables） 57
5.2.3 电子邮件通知变量 58

第 6 章 使用 Tripwire 软件 60

6.1 配置文件（Configuration file） 61
6.1.1 编辑配置文件 61
6.1.2 测试 E-mail 收发 61
6.1.3 定制默认的策略文件 62
6.1.4 初始化数据库 62
6.2 常规操作 63
6.2.1 完整性检测 63
6.2.2 检验报告文件 64
6.2.3 升级数据库 64
6.2.4 升级策略文件 65
6.2.5 修改密码短语（Passphrases） 65

第 7 章 认识 AIDE 68

7.1 了解 AIDE 69
7.1.1 AIDE 的功能 69
7.1.2 AIDE 安装要求 70

7.1.3 基本用法 70
7.1.4 工作流程图 71
7.1.5 AIDE 的最新版本 71
7.2 编译安装 72
7.2.1 源代码验证 72
7.2.2 利用 MD5 检查 73
7.2.3 configure 配置 73
7.2.4 configure 参数 73
7.2.5 编译和安装 76
7.2.6 编写配置文件 76
7.2.7 配置文件实例 76
7.2.8 AIDE 安装后的目录 77
第 8 章 使用 AIDE 79
8.1 aide 命令 80
8.1.1 aide 命令的 5 种工作模式 80
8.1.2 相关参数 82
8.1.3 错误信息 83
8.1.4 相关文件 83
8.2 配置文件 84
8.2.1 了解配置文件 84
8.2.2 调试配置文件 86
8.2.3 文件格式比较 86
8.3 理解 AIDE 规则 86
8.3.1 规则结构 87
8.3.2 Aide 规则配置算法 87
8.4 配置语句 87
8.4.1 配置语句（config lines） 87
8.4.2 变量 88
8.4.3 符号 “+” 和 “-” 的使用 90
8.4.4 AIDE 的检测类型 90
8.5 AIDE 中的宏定义 93
8.5.1 宏语句 93

8.5.2 语法解释 93
8.6 选择语句 94
8.6.1 选择语句类型 94
8.6.2 符号“!”和“$”的使用 94
8.7 数据库和配置文件的校验签名 95
8.7.1 相关的 configure 参数 95
8.7.2 建立校验签名的数据库和配置文件 96
8.7.3 使用校验签名的意义 97
8.8 实验 98
第 9 章 使用 ICU 100
9.1 了解 ICU 101
9.1.1 ICU 的工作原理 101
9.1.2 安装 ICU 的要求 102
9.2 编译和安装 102
9.2.1 安装 ICU 服务器 102
9.2.2 关于使用 AIDE 的两点说明 106
9.2.3 SSH 的两个版本 107
9.3 默认配置文件的注解 110
9.4 ICU.pl 命令 116
9.4.1 一般模式（General usage） 116
9.4.2 体检模式（Sanity check） 117
9.4.3 密钥生成模式（Key generation） 117
9.4.4 ICU.pl 的另外两个参数 118
9.5 使用 ICU 118
9.5.1 在 ICU 服务器端添加客户端 118
9.5.2 客户端在远程主机上的安装 119
9.5.3 在服务器端对客户端的操作 121
9.5.4 服务器端的计划工作 122
9.5.5 关于服务器端及客户端的数据库文件 122
9.5.6 关于服务器端的日志文件 124
9.5.7 关于邮件的内容 124
9.5.8 使用后的安装目录 126

9.5.9 使用中的注意事项 127
9.6 实验 128

中篇 Linux 下病毒的防治

第 10 章 Clam AntiVirus 132

10.1 Clam AntiVirus 概论 133
10.2 编译安装 clamAV 134
10.3 CVD 格式 135
10.3.1 分析 CVD 格式 136
10.3.2 签名格式（Signature formats） 137
10.3.3 签名名字（Signature names） 142
10.3.4 三类特殊文件的签名 143
10.3.5 自定义数据库 144

第 11 章 Clamd 服务器 146

11.1 安装 ClamAV 147
11.2 定制配置文件 147
11.3 与其他服务结合 147
11.4 相关的配置文件 147
11.4.1 clamd.conf 配置文件格式 147
11.4.2 freshclamconf 配置文件格式 166

第 12 章 Clamd 与用户文件系统 174

12.1 ClamFS 用户文件系统 175
12.1.1 安装要求 175
12.1.2 ClamFS 文件系统原理 175
12.1.3 功能 176
12.1.4 内部组织结构 176
12.1.5 ClamFS 的简化流程图 176
12.1.6 编译安装 177
12.1.7 安装后的文件结构 177
12.1.8 ClamFS 命令 177
12.1.9 配置文件 178

12.1.10 启动 ClamFS 179
12.1.11 使用 ClamFS 文件系统 180
12.1.12 关闭 ClamFS 进程 181
12.2 Dazuko 181
12.2.1 概述 Dazuko 181
12.2.2 下载并安装 Dazuko 181
12.2.3 Dazuko 与 ClamAV 的结合 184
12.2.4 测试 185
12.3 Clamuko 186
12.3.1 打开 Clamuko 功能 186
12.3.2 设置保护目录 187
12.3.3 测试 187
12.4 Dazukofs 187
12.4.1 概述 Dazukofs 188
12.4.2 示意图 188
12.4.3 源文件目录结构 189
12.4.4 编译安装 189
12.4.5 设置 Clamuko 193

第 13 章 Linux 下的服务与 ClamdAV 197

13.1 Apache 与 Clamd 198
13.1.1 概述 198
13.1.2 安装要求 198
13.1.3 编译安装 198
13.1.4 配置 mod_clamav 199
13.1.5 测试 mod_clamav 204
13.2 Proftp 与 Clamd 209
13.2.1 概述 209
13.2.2 编译安装 210
13.2.3 mod_clamav 的配置 211
13.2.4 抗病毒功能测试 212
13.3 Samba 与 ClamAV 213
13.3.1 概述 213

13.3.2 下载并安装 Samba 213
13.3.3 安装 samba-vscan 214
13.3.4 配置文件 214
13.3.5 运行 samba 及 clamd 进程 216
13.3.6 检查日志看启动情况 216
13.3.7 抗病毒功能测试 217
13.4 Squid 与 ClamAV 218
13.4.1 概述 218
13.4.2 编译安装 219
13.4.3 HAVP 与 Squid 进行结合 229
13.4.4 启动 HAVP 230
13.4.5 测功能试 230
13.4.6 设置 HAVP 以服务模式启动 231
13.4.7 相关文件 blacklist 和 whitelist 232
13.5 Postfix 与 ClamAV 233
13.5.1 认识 amavisd-new 233
13.5.2 安装 amavisd-new 236
13.5.3 整合 Postfix 和 amavisd-new 253
13.5.4 整合 Postfix 和 amavisd-new 实例 267
13.5.5 其他命令 273
第 14 章 监控与管理 Clamd 278
14.1 clamd 启动脚本（init script） 279
14.2 监控与自动重启 clamd 280
14.2.1 clamdmon 工具 280
14.2.2 clamdwatch 工具 282
14.3 clamd 相关命令 284
14.3.1 clamd 284
14.3.2 clamconf 286
14.3.3 clamdscan 288
14.3.4 clamdtop 290
14.3.5 clamscan 294
14.3.6 freshclam 299

14.3.7 sigtool.....301
14.3.8 clamav-config.....303

下篇 恢复人为删除的文件

第 15 章 对 ext3 下的文件恢复.....306

15.1 下载并安装 ext3grep.....307
15.2 恢复认为损坏的文件.....309
15.2.1 ext3 如何存储文件.....309
15.2.2 手动恢复举例.....330
15.2.3 恢复多个文件.....334

第 16 章 对 ext4 下的文件恢复.....338

16.1 了解 ext4.....339
16.2 下载并安装 extundelete 软件.....340
16.2.1 下载 extundelete.....340
16.2.2 安装相关软件.....340
16.3 了解 extundelete.....342
16.4 手动恢复举例.....349

LINUX

上篇　文件完整性

第 1 章　Tripwire 软件简介
第 2 章　Tripwire 的安装与部署
第 3 章　Tripwire 软件命令参考
第 4 章　策略参考
第 5 章　配置文件参考
第 6 章　使用 Tripwire 软件
第 7 章　认识 AIDE
第 8 章　使用 AIDE
第 9 章　使用 ICU

LINUX

第1章 Tripwire 软件简介

这一章是专门为没有接触过 Tripwire 软件的系统管理员，或者是不熟悉完整性评估（integrity assessment）的人而准备的，有经验的 Tripwire 用户可以直接跳过本章。

本章涵盖了以下内容。

Tripwire 软件的定义

Tripwire 软件的部署

Tripwire 软件的组成和安全功能

Tripwire 软件的工作机制

Tripwire 软件的应用