

## <<Solaris安全手册>>

### 图书基本信息

书名：<<Solaris安全手册>>

13位ISBN编号：9787115087287

10位ISBN编号：7115087288

出版时间：2000-10

出版时间：人民邮电出版社 (2000年10月1日)

作者：PeterH.Gregory

页数：253

字数：419

译者：潇湘工作室

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<Solaris安全手册>>

### 内容概要

本书从各个方面介绍如何保护Solaris系统的安全性。

全书共分为5部分，第一部分介绍安全性的基础知识，主要分析了安全问题的起因，并提出了系统安全的9大原则；第二部分介绍Solaris单机系统的安全保护，主要涉及到系统的启动与关闭、系统日志、用户帐号和环境、文件系统等内容；第三部分详述Solaris网络系统的安全保护，其主要内容有网络接口服务、网络打印、电子邮件、网络访问控制、名称服务等；第四部分介绍灾难恢复的问题；第五部分是附录。

本书适用于安全管理员和UNIX系统管理员。

## <<Solaris安全手册>>

### 书籍目录

#### 第一部分 安全性简介

##### 第1章 安全问题

###### 1.1 安全缺陷的起因

###### 1.1.1 网络连通性的增长

###### 1.1.2 软件的脆弱性

###### 1.1.3 雇员和承包商

###### 1.1.4 目的明确而足智多谋的黑客

###### 1.1.5 站点策略

##### 第2章 安全策略

###### 2.1 原则1：侵入系统的黑客很可能是认识的人

###### 2.2 原则2：不要轻信任何人，对必须要相信的人也要小心

###### 2.3 原则2a：不要过分自信，对每件事情都要确认

###### 2.4 原则3：要使潜在的侵入者相信他们会被抓住

###### 2.5 原则4：分层保护

###### 2.6 原则5：设计安全策略时要假设任何一个保护层完全失效的情况

###### 2.7 原则6：把安全性作为最初设计的一部分

###### 2.8 原则7：禁用不需要的服务、软件包和功能

###### 2.9 原则8：连接网络之前要想清楚并进行保护

###### 2.10 原则9：为最坏的情况做准备

###### 2.11 9个原则：一种生活方式

#### 第二部分 独立的系统

##### 第3章 PROM、OpenBoot和物理安全性

###### 3.1 什么是PROM

###### 3.2 什么是OpenBoot

###### 3.2.1 为什么绝对不能让用户接触OpenBoot

###### 3.2.2 通过设置安全参数来保护OpenBoot

###### 3.2.3 改变OpenBoot安全级别的过程

###### 3.2.4 丢失了所有口令--部分恢复过程

###### 3.2.5 推荐的启动设备

###### 3.2.6 改变OpenBoot徽标

###### 3.2.7 恢复丢失的超级用户口令

###### 3.3 系统物理安全性考虑因素

###### 3.3.1 防止偷窃和访问

###### 3.3.2 审查PROM

###### 3.3.3 OpenBoot口令

###### 3.3.4 CD-ROM驱动器

###### 3.3.5 备份介质

###### 3.3.6 操作系统版本介质

###### 3.4 补充信息

##### 第4章 文件系统

###### 4.1 什么是文件系统

###### 4.1.1 有些应用程序需要开放的权限

###### 4.2 理解文件和目录的权限

###### 4.2.1 身份：用户、组及其他

###### 4.2.2 权限总结：读、写、执行、SetUID、SetGID、粘着位

## <<Solaris安全手册>>

- 4.3 小结：身份和权限
- 4.4 查看文件和目录权限的方式
  - 4.4.1 权限：数值形式
  - 4.4.2 设置文件和目录的权限--数值形式
  - 4.4.3 设置文件和目录的权限--符号形式
- 4.5 umask及其工作方式
  - 4.5.1 Ksh和umask -S
  - 4.5.2 默认的文件权限和umask
  - 4.5.3 超级用户的umask
  - 4.5.4 默认的目录权限和umask
  - 4.5.5 如何查找具有指定权限设置的文件
- 4.6 系统设备访问权限
- 4.7 文件系统审核工具
  - 4.7.1 ASET
  - 4.7.2 COPS
  - 4.7.3 Tiger
  - 4.7.4 Tripwire
  - 4.7.5 lsof ( 列出打开的文件 )
- 4.8 其他安全工具和技术
  - 4.8.1 检查/etc/权限
  - 4.8.2 保证正确的utmp和utmpx权限
  - 4.8.3 使用固定模式工具增强安全性
  - 4.8.4 使用fuser命令
  - 4.8.5 使用ls命令显示隐藏的文件和文件名中隐藏的字符
  - 4.8.6 为ls命令取别名
  - 4.8.7 为rm命令取别名
  - 4.8.8 用fsirand使文件系统I节点号随机化
  - 4.8.9 文件系统配额
- 4.9 文件系统访问控制表
- 4.10 补充信息
- 第5章 用户帐号和环境
  - 5.1 简介
  - 5.2 用户帐号安全
    - 5.2.1 超级用户帐号
    - 5.2.2 其他管理性的帐号和组
    - 5.2.3 用户帐号
    - 5.2.4 用户何时需要超级用户特权
    - 5.2.5 PATH和LD\_LIBRARY\_PATH
  - 5.3 口令文件、影像文件和组文件
    - 5.3.1 口令文件
    - 5.3.2 影像文件
    - 5.3.3 口令安全
    - 5.3.4 UNIX组
    - 5.3.5 /etc/default/passwd文件
  - 5.4 成为超级用户
    - 5.4.1 直接以超级用户登录
    - 5.4.2 su命令

## <<Solaris安全手册>>

### 5.5 外壳和应用程序的安全性

#### 5.5.1 强制启动应用程序

#### 5.5.2 在超级用户的外壳提示符中包含系统名称

#### 5.5.3 受限制的外壳

#### 5.5.4 默认的登录环境

#### 5.5.5 直接写控制台

#### 5.5.6 程序缓冲区溢出

#### 5.5.7 其他进程信息

### 5.6 X-Windows安全性

#### 5.6.1 X-Windows屏幕手工锁定

#### 5.6.2 X-Windows屏幕自动锁定

#### 5.6.3 X-Windows显示器权限

### 5.7 审核工具

#### 5.7.1 COPS

#### 5.7.2 Crack

### 5.8 补充信息

## 第6章 系统启动和关闭

### 6.1 系统运行级别

#### 6.1.1 确定当前运行级别

### 6.2 系统启动

#### 6.2.1 PROM

#### 6.2.2 多用户模式

#### 6.2.3 rc机制

### 6.3 系统关闭

#### 6.3.1 init

#### 6.3.2 uadmin

### 6.4 关于rc文件的更多信息

#### 6.4.1 分析rc文件的例子

### 6.5 审核启动和关闭机制

#### 6.5.1 COPS

#### 6.5.2 Tripwire

### 6.6 修改启动和关闭机制

#### 6.6.1 添加启动和关闭脚本

#### 6.6.2 改变启动和关闭脚本

#### 6.6.3 禁用启动和关闭脚本

#### 6.6.4 关于链接的启动文件的更多信息

### 6.7 补充信息的位置

## 第7章 cron和at

### 7.1 cron

#### 7.1.1 什么是cron

#### 7.1.2 cron如何工作

#### 7.1.3 如何配置cron

#### 7.1.4 cron用户配置

#### 7.1.5 用户访问cron系统

### 7.2 at

#### 7.2.1 什么是at

#### 7.2.2 at如何工作

## <<Solaris安全手册>>

### 7.2.3 用户访问at系统

### 7.3 应该避免的常见问题

#### 7.3.1 没有充分屏蔽cron运行的程序

#### 7.3.2 将crontab文件留在所有用户都可以看到的地方

#### 7.3.3 cron运行的脚本中存在不安全的PATH

#### 7.3.4 cron运行的脚本中存在不确定的PATH

#### 7.3.5 在cron和at作业中使用标准输入和标准输出

### 7.4 审核工具

#### 7.4.1 Tripwire

#### 7.4.2 COPS

### 7.5 补充信息

## 第8章 系统日志

### 8.1 什么是系统日志

### 8.2 syslog

#### 8.2.1 syslog的功能和安全级别

#### 8.2.2 syslog消息分类所用的表示法

#### 8.2.3 syslog配置

#### 8.2.4 调试syslog

### 8.3 loginlog

### 8.4 sulog

### 8.5 上一次登录

### 8.6 卷管理器日志

### 8.7 安装日志

### 8.8 sysidtool日志

### 8.9 帮助日志记录的工具--Logcheck

### 8.10 补充信息

## 第三部分 网络连接系统

## 第9章 网络接口和网络服务

### 9.1 网络

### 9.2 网络接口

#### 9.2.1 网络接口特性

### 9.3 网络接口配置

#### 9.3.1 ifconfig

#### 9.3.2 ndd

#### 9.3.3 利用/etc/notrouter关闭IP转发

#### 9.3.4 配置网络适配器

#### 9.3.5 混合模式

### 9.4 网络服务

#### 9.4.1 非必须的服务

#### 9.4.2 网络服务号

#### 9.4.3 网络服务配置

#### 9.4.4 网络服务的启动方式

#### 9.4.5 Daemon网络服务不和inetd一起启动

### 9.5 路由

#### 9.5.1 增加静态路由

#### 9.5.2 增加动态路由

### 9.6 使用snoop

## <<Solaris安全手册>>

### 9.7 补充信息

### 第10章 网络/系统体系结构

#### 10.1 什么是体系结构

#### 10.2 简单和复杂体系结构的比较

#### 10.3 体系结构原理

##### 10.3.1 原理1：最小化故障点数目（或者缩短关键路径）

##### 10.3.2 原理2：把服务尽量设置在靠近它们所服务对象的位置

##### 10.3.3 原理3：将服务和对应的应用程序纵向对齐

##### 10.3.4 原理4：准备为网络增加分区

### 第11章 电子邮件

#### 11.1 电子邮件概述

##### 11.1.1 传输代理

##### 11.1.2 递送代理

##### 11.1.3 用户代理

#### 11.2 电子邮件安全性弱点的类型

##### 11.2.1 Auth（或Identd）协议

##### 11.2.2 邮件代理程序

##### 11.2.3 消息源路由

##### 11.2.4 隐私

##### 11.2.5 可信性

#### 11.3 减轻电子邮件的安全性问题

##### 11.3.1 只在电子邮件服务器上运行sendmail

##### 11.3.2 断开内部邮件服务器与Internet的直接连接

##### 11.3.3 禁止带有路由信息的邮件

##### 11.3.4 实现邮件加密和数字签名

##### 11.3.5 替代Sendmail

##### 11.3.6 删除不必要的电子邮件别名

##### 11.3.7 实现Smrsh

##### 11.3.8 实现ForwardPath

#### 11.4 补充信息

### 第12章 打印

#### 12.1 打印体系结构

#### 12.2 打印子系统目录

##### 12.2.1 审核打印子系统的目录

#### 12.3 本地打印

##### 12.3.1 本地打印设备

##### 12.3.2 确定打印机使用的设备

##### 12.3.3 打印设备访问权限

##### 12.3.4 审核打印设备权限

#### 12.4 限制对打印机和打印服务器的访问

##### 12.4.1 直接访问网络打印机

#### 12.5 补充信息

### 第13章 网络访问控制

#### 13.1 网络访问控制原理

##### 13.1.1 不必要的网络访问点是对安全性的威胁

##### 13.1.2 没有防备的网络接入点是对安全性的威胁

#### 13.2 必须的和非必须的服务

## <<Solaris安全手册>>

- 13.2.1 如何停止运行非必须的服务
- 13.2.2 禁止在/etc/inet/services和/etc/inet/inetd.conf文件中没有定义的服务
- 13.3 加强网络访问控制
  - 13.3.1 inetd连接跟踪
  - 13.3.2 TCP Wrapper
  - 13.3.3 公共域rpcbind
  - 13.3.4 .rhosts文件??r-命令的网关
  - 13.3.5 /etc/hosts.equiv文件
  - 13.3.6 审核.rhosts和hosts.equiv文件
  - 13.3.7 对telnet、rsh和rlogin的安全替换
  - 13.3.8 X-Windows是不安全的
  - 13.3.9 防火墙
- 13.4 测试系统的辅助选项
  - 13.4.1 Satan
  - 13.4.2 ISS
- 13.5 检测非法入侵
  - 13.5.1 Syn
  - 13.5.2 Klaxon
  - 13.5.3 Courtney
  - 13.5.4 Tocsin
  - 13.5.5 Gabriel
  - 13.5.6 非法入侵检测：紧跟潮流
- 13.6 身份验证
  - 13.6.1 系统身份验证
  - 13.6.2 DES (Diffie-Hellman)身份验证
  - 13.6.3 Kerberos身份验证
- 13.7 虚拟专用网
  - 13.7.1 SKIP
  - 13.7.2 IPsec
- 13.8 补充信息
- 第14章 域名服务
  - 14.1 域名服务DNS
    - 14.1.1 /etc/nsswitch.conf
    - 14.1.2 /etc/resolv.conf
  - 14.2 DNS的安全性漏洞和解决方案
    - 14.2.1 在Internet上暴露太多的信息
    - 14.2.2 DNS服务器的非法区域传输
    - 14.2.3 Nslookup和真正的DNS请求之间的区别
    - 14.2.4 公共域DNS ( BIND )
    - 14.2.5 DIG公共域工具
    - 14.2.6 禁止nscd缓存
    - 14.2.7 了解BIND的版本
  - 14.3 NIS
    - 14.3.1 获取并安装NISKIT
  - 14.4 NIS安全性漏洞和解决方案
    - 14.4.1 将NIS映射从/etc目录中转移出去
    - 14.4.2 保护NIS映射目录



## <<Solaris安全手册>>

- 14.4.3 使用难以猜到的NIS域名
- 14.4.4 实现/var/yp/securenets
- 14.4.5 隐藏影像域
- 14.4.6 避免使用非法NIS服务器
- 14.4.7 不要将根帐号和其他管理帐号包含在NIS中
- 14.4.8 禁止nscd缓存
- 14.4.9 其他NIS安全性漏洞
- 14.5 NIS+
- 14.5.1 NIS+的默认访问权限
- 14.5.2 主类nobody的访问权限
- 14.5.3 NIS+安全性级别
- 14.5.4 NIS+管理
- 14.5.5 备份NIS+表
- 14.5.6 刷新NIS+事务处理记录
- 14.5.7 不要将根帐号和其他管理帐号包含在NIS+中
- 14.5.8 禁止nscd缓存
- 14.6 域名服务开关
- 14.7 Nscd
- 14.8 补充信息
- 第15章 NFS和Automounter
- 15.1 NFS
- 15.1.1 NFS操作
- 15.1.2 提高NFS共享的安全性
- 15.1.3 提高NFS装入的安全性
- 15.1.4 通过设置Portmon提高NFS的安全性
- 15.1.5 NFS身份验证
- 15.1.6 服务器作为NFS客户机
- 15.1.7 NFS和访问控制列表
- 15.1.8 网络上的NFS
- 15.1.9 禁止NFS
- 15.2 Automounter
- 15.2.1 间接Automounter映射
- 15.2.2 直接Automounter映射
- 15.2.3 Automounter浏览
- 15.2.4 Automounter和域名服务开关
- 15.2.5 禁止Automounter
- 15.3 补充信息
- 第四部分 事故和恢复
- 第16章 系统恢复的准备工作
- 16.1 故障因素
- 16.1.1 自然灾害
- 16.1.2 人为灾害
- 16.1.3 内部设施故障
- 16.1.4 硬件故障
- 16.1.5 UNIX管理员失误
- 16.1.6 文档错误
- 16.1.7 程序员失误

## <<Solaris安全手册>>

- 16.1.8 用户失误
- 16.1.9 有意破坏
- 16.2 为系统恢复作准备
  - 16.2.1 成立事故反应小组
  - 16.2.2 系统的文件系统设计
  - 16.2.3 文件系统的几何结构
  - 16.2.4 磁带备份
  - 16.2.5 系统恢复测试
  - 16.2.6 软件版本的存储介质
  - 16.2.7 系统事件日志
  - 16.2.8 Solaris和工具软件的补丁程序
  - 16.2.9 CD-ROM驱动器
  - 16.2.10 硬件和软件服务协议
  - 16.2.11 保留硬件的备用件
  - 16.2.12 关键服务器PROM的备份
  - 16.2.13 备用的磁盘空间
  - 16.2.14 恢复文档
  - 16.2.15 联系和交叉培训 ( Cross-Training )
- 16.3 内部伙伴
- 16.4 外部伙伴
- 16.5 补充信息
- 第五部分 附录
- 附录A 安全性信息的在线资源
  - A.1 安全性Web站点
  - A.2 黑客Web站点
  - A.3 安全性邮寄列表
  - A.4 补丁程序
- 附录B 公共域安全工具的在线资源
  - B.1 TCP/IP安全性工具
    - B.1.1 ISS ( Internet security scan , 安全性扫描 )
    - B.1.2 Satan ( Security Administrators Tool for Analg Zing Networks , 分析网络的安全性管理工具 )
    - B.1.3 Cpm ( check promiscuous mode , 检查混杂模式 )
    - B.1.4 tcpdump ( network monitoring and data acquisition , 网络监视和数据采集 )
  - B.2 访问控制安全工具
    - B.2.1 TCP Wrappers
    - B.2.2 rpcbind
    - B.2.3 Ssh ( secure shell , 安全外壳 )
    - B.2.4 Kerberos
    - B.2.5 crack ( password cracker , 口令快客 )
    - B.2.6 fwtk ( fire wall toolkit , 防火墙工具 )
    - B.2.7 S/Key
  - B.3 侵入检测工具
    - B.3.1 Klaxon
    - B.3.2 Courtney
    - B.3.3 Tocsin
    - B.3.4 Gabriel

## <<Solaris安全手册>>

- B.3.5 syn
- B.4 文件系统安全性工具
  - B.4.1 Tiger
  - B.4.2 Tripwire
  - B.4.3 COPS
- B.5 加密工具
  - B.5.1 PGP
  - B.5.2 MD5
- B.6 电子邮件安全性工具
  - B.6.1 SMAP ( sendmail wrapper , sendmail包装 )
  - B.6.2 sendmail V8 ( Public-domain Sendmail, 公共域发送邮件 )
  - B.6.3 Postfix ( formerly Vmailer , 以前的Vmailer )
  - B.6.4 smrsh
- B.7 DNS工具
  - B.7.1 公共域BIND
  - B.7.2 Dig
  - B.7.3 其他DNS工具
- B.8 其他工具和资源
  - B.8.1 Logcheck
  - B.8.2 lsof ( list open files , 开放文件列表 )
  - B.8.3 Patchdiag
  - B.8.4 fix-modes
  - B.8.5 perl
  - B.8.6 Washington大学ftpd
- B.9 安全性工具站点
  - B.9.1 CERT工具
  - B.9.2 CIAC工具
  - B.9.3 COAST工具
  - B.9.4 Doug工具
  - B.9.5 LIST ( 信息安全技术实验室 ) 安全性工具
  - B.9.6 Sun免费软件站点
  - B.9.7 Wietse Venema的UNIX安全性工具集
- B.10 黑客工具站点
- 附录C 获得和应用Solaris补丁程序
  - C.1 补丁信息的来源
  - C.2 理解Solaris补丁程序
  - C.3 理解Solaris补丁集
  - C.4 补丁程序的来源
  - C.5 补丁程序安装策略
    - C.5.1 安装补丁程序之前
    - C.5.2 要安装的补丁程序
    - C.5.3 测试补丁程序
    - C.5.4 为补丁程序重新引导系统
    - C.5.5 patchdiag程序
    - C.5.6 补丁程序安装程序 , Solaris 2.x-2.5.1
    - C.5.7 Solaris 2.6和Solaris 7的补丁程序安装过程
    - C.5.8 Solaris OS升级

## <<Solaris安全手册>>

C.6 补充信息

附录D 推荐读物

D.1 参考书

D.2 在线出版物和文章

D.3 SunSolve出版物

D.4 在线期刊

D.5 Internet RFC

附录E Solaris安全产品

E.1 SunScreen ETS

E.2 SunScreen SPF

E.3 SunScreen SKIP

E.4 Sun Security Manager

E.5 SunScreen SecureNet

E.6 Trusted Solaris

E.7 补充信息

附录F 实现C2安全措施

F.1 什么是C2安全措施

F.2 C2安全措施的代价

F.3 启用C2安全措施

F.4 禁用C2安全措施

F.5 管理C2安全措施

F.5.1 C2审核捕获的配置

F.5.2 C2日志的管理

F.5.3 性能的管理

F.5.4 审核事件

F.5.5 审核跟踪分析

F.5.6 可移动存储介质管理

F.5.7 设备安置

F.5.8 建议

F.6 补充信息

附录G 验证公共域软件的完整性

G.1 使用PGP验证

G.2 使用MD5的验证

G.3 获得补充信息

附录H 攻击词汇表

附录I 保护系统安全检查表

## <<Solaris安全手册>>

### 版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>