<<Linux安全>>

图书基本信息

书名：<<Linux安全>>

13位ISBN编号：9787111093831

10位ISBN编号：7111093836

出版时间：2002-1

出版时间：机械工业出版社

作者：BobToxen

页数：517

<<Linux安全>>

内容概要

本书介绍Linux系统安全维护的技术。
主要内容包括：一般性安全问题、高级安全问题、安全策略、信任机制以及猝发入侵和最近的入侵方法，如何为入侵做准备，如何进行入侵检测，如何成功、安全、快速地从遇到的入侵中进行恢复等。
本书内容丰富、章节安排合理，适合广大Linux或UNIX系统管理员以及对安全方面感兴趣的读者阅读。
附带光盘包括安全性监视工具软件。

<<Linux安全>>

书籍目录

译者序
序言
第1章 导言
1.1 本书适合的读者
1.2 本书的组织结构
1.2.1 本书的约定
1.2.2 背景
1.3 需要防范的内容
1.4 谁是你的敌人
1.5 他们想干什么
1.6 保护与入侵的代价
1.7 硬件保护
1.8 对网络和调制解调器的访问进行保护
1.9 对系统的访问进行保护
1.10 文件保护
1.11 针对入侵的准备和检测
1.12 从入侵中恢复
第一部分 保 护 系 统
第2章 常见问题的快速解决
2.1 了解Linux安全性
2.1.1 Linux系统的安全性
2.1.2 攻击路径
2.1.3 进入安全环
2.2 七种致命错误
2.2.1 脆弱的口令
2.2.2 开放网络端口
2.2.3 旧软件版本
2.2.4 很差的物理安全性
2.2.5 不安全的CGI
2.2.6 陈旧的和不必要的账户
2.2.7 耽搁
2.3 良好安全性的重点：口令
2.4 先进的口令技术
2.4.1 可以获得很好的安全性的隐蔽的MD5口令
2.4.2 口令的重复提示
2.4.3 口令应该是成熟的吗
2.4.4 账户名
2.5 防止系统中的用户操作错误
2.5.1 引入软件的危险
2.5.2 教育用户
2.6 限制访问权限
2.6.1 目录与粘着位
2.6.2 找出权限问题
2.6.3 在启动脚本中使用U掩码
2.7 初始系统安装中的危险和干扰

2.8 限制不合理的访问
2.8.1 限制根用户可以登录的终端
2.8.2 拨打完整序列的电话号码
2.8.3 停止对数据不受控制的访问
2.8.4 限制服务器的接口
2.9 防火墙和公司其他的防范措施
2.9.1 停止终端在防火墙周围运行
2.9.2 开隧道通过防火墙
2.9.3 更改内核设置
2.9.4 Egress过滤
2.9.5 局域网隐患
2.9.6 公司内部的防火墙存在隐患
2.10 关掉不必要的服务
2.11 高安全性要求最小数量的服务
2.12 不再使用有隐患的服务
2.12.1 不要使用finger
2.12.2 关掉rwhod
2.12.3 关掉rwalld
2.12.4 关掉SNMP
2.12.5 关掉NFS、mountd和portmap
2.12.6 转换NFS在TCP上运行
2.12.7 关掉rsh、rcp、rlogin和rexec
2.12.8 关掉fdmount
2.12.9 关掉Echo和Chargen
2.12.10 关掉talk和ntalk
2.12.11 关掉TFTP
2.12.12 关掉systat和netstat
2.12.13 关掉内部的inetd服务
2.12.14 升级updatedb和locate
2.13 用新版本代替旧版本
2.13.1 升级named程序
2.13.2 升级2.2内核
2.13.3 升级sendmail
2.13.4 加强Sendmail来抵御DoS攻击
2.13.5 升级SSH
2.13.6 升级WU-FTPD
2.13.7 升级Netscape
2.13.8 禁止Web广告
2.13.9 升级mountd
2.13.10 升级gpm
2.13.11 升级imwheel
2.13.12 升级OpenLDAP
2.13.13 修正OpenLDAP
2.13.14 修正innd
2.13.15 Postgresql的脆弱之处
2.14 把不同安全等级的服务分隔开
第3章 简单入侵方法及应对策略

3.1 X系统的安全漏洞
3.2 物理入侵
3.2.1 从入侵者的软盘或光盘启动系统
3.2.2 CMOS重新配置
3.2.3 给CMOS加上密码
3.2.4 防止未授权用户使用单用户模式
3.2.5 防止用软盘窃取信息
3.2.6 防止Ctrl-Alt-Delete组合键的袭击
3.3 其他主题
3.3.1 电缆调制解调器
3.3.2 $PATH中“.”引发的问题
3.3.3 阻塞IP源路由
3.3.4 阻塞IP欺骗
3.3.5 屏幕自动锁定
3.3.6 /etc/mailcap
3.3.7 chattr程序和不可修改标志位
3.3.8 安全删除
3.3.9 同步I/O
3.3.10 用以增强安全性的mount参数
3.3.11 使用SSH包装UDP和TCP
3.3.12 cat目录与man命令
3.3.13 用*limit限制资源使用
3.3.14 公共界面下shell程序的历史记录
3.3.15 理解地址解析协议
3.3.16 防止ARP缓存中毒
3.3.17 Shell转义
3.3.18 你自己的ISP
3.3.19 终端探测程序
3.3.20 Star Office
3.3.21 VMware
3.4 终端设备攻击
3.4.1 功能键劫持
3.4.2 组合键的脆弱之处
3.4.3 xterm修改日志文件的脆弱之处
3.5 磁盘探测
3.5.1 真正擦除文件
3.5.2 破坏在空闲数据块上的旧的保密数据
3.5.3 擦除整个磁盘上的数据
3.5.4 破坏一个硬盘
第4章 入侵子系统的一般方法
4.1 NFS、mountd以及portmap
4.2 Sendmail
4.2.1 分离或多邮件服务器的附加安全性
4.2.2 Sendmail基础安全性
4.2.3 Sendmail安全选项
4.2.4 伪造邮件及新闻发送者地址
4.2.5 垃圾邮件来自何处

4.2.6 转发垃圾邮件
4.2.7 阻塞垃圾邮件
4.2.8 抵制垃圾邮件的工具
4.2.9 启用控制中继功能
4.2.10 禁止公开邮递列表
4.2.11 写满磁盘的Sendmail DoS
4.3 Telnet
4.4 FTP
4.4.1 匿名FTP的配置
4.4.2 FTP代理威胁
4.5 rsh、rcp、rexec以及rlogin服务
4.5.1 R*安全性
4.5.2 R*的不安全性
4.6 DNS
4.6.1 限制由于升级Named所带来的损害
4.6.2 服务于人
4.7 POP及IMAP服务器
4.8 使用Samba
4.8.1 Samba是否在系统上
4.8.2 Samba的卸载
4.8.3 Samba配置文件
4.8.4 文件smb.conf
4.8.5 注意CIFS／SMB-Only的用户
4.9 防止使用Squid来覆盖入侵痕迹
4.10 syslogd服务
4.11 print服务
4.12 ident服务
4.13 INND与News
4.14 保护你的DNS注册
第5章 常见攻击方法
5.1 Rootkit攻击
5.2 报文欺骗
5.2.1 为何UDP报文欺骗得以成功
5.2.2 TCP顺序号欺骗
5.2.3 会话劫持
5.3 SYN泛洪攻击
5.4 阻止SYN泛洪攻击
5.5 阻止TCP顺序号欺骗
5.6 报文风暴、Smurf攻击和Fraggles
5.6.1 避免成为放大器
5.6.2 阻止报文风暴攻击
5.6.3 Cisco路由器
5.6.4 DDoS攻击：被抵消的网络资源
5.7 缓冲区溢出或使用get()标记内存
5.8 欺骗技术
5.8.1 邮件欺骗
5.8.2 MAC攻击

5.8.3 中毒的ARP缓存
5.8.4 中毒的DNS缓存
5.9 中间人攻击
第6章 高级安全问题
6.1 配置具有更高安全性的Netscape
6.1.1 Netscape的重要属性
6.1.2 获取自己的cookie
6.1.3 系统用户的Netscape首选
6.1.4 Netscape个人安全管理器
6.1.5 Netscape Java的安全性
6.2 终止对I/O设备的访问
6.2.1 为何/dev/tty的模式设为666
6.2.2 虚拟控制台缓冲区的脆弱之处
6.2.3 可加密的磁盘驱动程序
6.3 跟踪Apache安全问题
6.3.1 所有权和权限
6.3.2 SSI
6.3.3 ScriptAllias
6.3.4 防止用户改变系统设置
6.3.5 控制Apache可以访问的目录
6.3.6 控制Apache可以访问的文件扩展
6.3.7 杂项
6.3.8 数据库泄漏
6.3.9 拒绝不受欢迎的主机
6.3.10 到站点的链接
6.4 Web服务器使用的几种特殊技术
6.4.1 将多个服务互相隔离
6.4.2 切勿信任CGI
6.4.3 隐藏的表单变量与被破坏的Cookie
6.4.4 保护职员的个人信息
6.4.5 禁止Robot
6.4.6 危险的CGI程序
6.4.7 利用CGI Query程序的漏洞进行攻击
6.4.8 转换十六进制编码的URL
6.4.9 利用CGI Counterfiglet程序进行的攻击
6.4.10 利用CGI phf程序进行的攻击
6.4.11 CGI脚本和程序
6.4.12 强制URL封锁
6.4.13 探测被毁损的Web页
6.5 安全的信用卡数据单向传输
6.6 强化系统安全性
6.7 限制登录地点及次数
6.8 一些隐秘但致命的安全问题
6.8.1 防范缓冲区溢出攻击
6.8.2 防范chroot()攻击
6.8.3 符号链接攻击
6.8.4 lost+found=全部问题

6.8.5 rm -r 竞争
6.9 防止登录模拟器攻击
6.9.1 更新/etc/issue
6.9.2 弥补/bin/login
6.9.3 内核支持
6.10 使用Libsafe防止缓冲区溢出
第7章 创建安全策略
7.1 通用策略
7.2 个人使用策略
7.3 账户策略
7.4 电子邮件策略
7.5 Web服务器策略
7.6 文件服务器和数据库策略
7.7 防火墙策略
7.8 桌面策略
7.9 便携式电脑策略
7.10 报废策略
7.11 网络拓扑策略
7.12 问题报告策略
7.13 所有权策略
7.14 选择策略的策略
第8章 对其他机器的信任机制
8.1 安全系统与不安全系统
8.2 控制下的Linux系统和UNIX系统
8.3 控制主机
8.4 Windows的安全特征
8.5 防火墙的脆弱之处
8.6 虚拟专用网络
8.7 病毒与Linux
第9章 分段入侵
9.1 Mission Impossible技术
9.2 间谍
9.3 疯狂攻击和自杀性攻击
第10章 案例分析
10.1 Berkeley 防御系统的漏洞
10.2 这个领域中的佼佼者
10.3 Ken Thompson对海军的攻击
10.4 虚拟机特洛伊木马
10.5 AOL的DNS更改失败
10.6 “ 我是无辜的 ”
10.7 用笔记本电脑和付费电话进行攻击
10.8 从巨额数目中盗窃几美分
第11章 最新的入侵方法
11.1 分段攻击
11.2 死亡性Ping
11.3 秘密扫描
11.4 电缆调制解调器：一个黑客的梦

11.5 用Sendmail来阻止电子邮件攻击
11.6 Sendmail账户猜想
11.7 神秘的ingreslock
11.8 你正在被跟踪
11.8.1 Pentium III 序列号
11.8.2 Microsoft的GUID允许监视
11.9 分布式拒绝服务攻击
11.10 隐藏的特洛伊木马程序
11.10.1 为什么要用ICMP回应报文及如何回应
11.10.2 特洛伊木马将来的方向
11.10.3 混杂模式内核消息
11.11 经过TCP 98端口的Linuxconf
11.12 恶意的HTML标志和脚本
11.13 syslog（）的格式问题
第二部分 入侵防范准备
第12章 加固系统
12.1 用SSH保护用户会话
12.1.1 编译SSH2
12.1.2 配置SSH
12.1.3 使用SSH
12.1.4 用SSH包装X
12.1.5 使用SSH、PPP和Perl的VPN
12.1.6 使用sftp
12.1.7 使用scp
12.1.8 用SSH封装其他基于TCP的服务
12.1.9 使用FreeS/WAN IPSec建立VPN
12.1.10 SSH不能防范的脆弱之处
12.2 PGP
12.3 FSF的PGP替代软件
12.3.1 下载
12.3.2 编译
12.3.3 工作原理
12.3.4 生成密钥
12.3.5 交换密钥
12.3.6 传播你的公开密钥
12.3.7 签名文件
12.3.8 邮件的加密和签名
12.3.9 加密的备份和其他过滤器
12.3.10 非常高的GPG安全性
12.4 使用IP Chain和DMZ的防火墙
12.4.1 IP Chain不能做什么
12.4.2 IP Chain基础
12.4.3 IP Chain命令
12.4.4 启动一个防火墙脚本
12.4.5 防火墙的基本用法
12.4.6 阻塞外部恶意入侵
12.4.7 IP伪装

12.4.8 创建DMZ
12.4.9 有状态的防火墙
12.4.10 SSH危险
12.4.11 加密的邮件访问
第13章 硬件准备
13.1 时间就是一切
13.2 高级准备
13.3 切换到辅助控制
13.3.1 哪个系统应该具有备份系统
13.3.2 两类备份系统
13.3.3 安全备份系统设计
13.3.4 保持安全备份系统处于就绪状态
13.3.5 检查高速缓存
13.3.6 最好准备一个空闲的硬盘
第14章 配置准备
14.1 TCP Wrapper
14.1.1 TCP Wrapper的使用
14.1.2 TCP Wrapper的高级使用
14.2 自适应TCP Wrapper
14.3 Cracker Trap
14.3.1 /etc/service文件
14.3.2 /etc/inetd.conf文件
14.3.3 /etc/hosts.allow文件
14.4 用内核模式终止黑客服务器
14.5 应急训练
14.5.1 飞机失事演习
14.5.2 这只是一次测试
14.5.3 危险和预防
14.5.4 计划好进行哪些演习
14.5.5 测试系统
14.5.6 安全的特洛伊木马
14.5.7 程序的大小很重要
14.5.8 引起更多的麻烦
14.6 用Tiger team侵入你自己的系统
第15章 扫描系统
15.1 Nessus安全扫描程序
15.2 SARA和SAINT安全审计程序
15.3 nmap网络映射程序
15.4 Snort攻击检测程序
15.5 用SHADOW进行扫描和分析
15.6 John the Ripper
15.7 保存RPM数据库校验和
第三部分 入 侵 检 测
第16章 行为监视
16.1 日志文件
16.2 如何利用日志文件
16.3 当有人攻击系统时呼叫系统管理员

16.4 一个自动呼叫的例子
16.5 使用你的自动呼叫的例子
16.6 呼叫telnet和rsh的使用
16.7 监视端口的使用
16.8 使用tcpdump监视你的局域网
16.8.1 编译tcpdump
16.8.2 使用tcpdump
16.9 用欺骗工具包监视扫描程序
16.10 监视进程
16.11 使用cron来提防黑客
16.12 Caller ID
第17章 扫描系统查找异常
17.1 找出可疑的文件
17.1.1 分析可疑的文件
17.1.2 定期地比较文件内容
17.2 Tripwire
17.2.1 安装Tripwire
17.2.2 使用Tripwire
17.2.3 Tripwire不能保护什么
17.2.4 Tripwire的替代程序
17.3 检测删除的可执行文件
17.4 检测混杂模式的网络接口卡
17.5 找出混杂的进程
17.6 自动检测被涂改的Web页面
第四部分 入 侵 恢 复
第18章 重新获得对系统的控制
18.1 找到黑客运行的进程
18.2 处理运行着的黑客进程
18.3 断开调制解调器、网络、打印机和系统
第19章 找出并修复损害
19.1 检查/var/log日志
19.2 syslogd和klogd守护进程
19.3 远程记录
19.4 解释日志文件项
19.4.1 lastlog
19.4.2 messages
19.4.3 syslog
19.4.4 kernlog
19.4.5 cron
19.4.6 xferlog
19.4.7 daemon
19.4.8 mail
19.5 检查其他日志
19.6 检查TCP Wrapper
19.7 文件系统被怎样破坏
19.8 植入假的数据
19.9 修改了的监视程序

19.10 什么都不可信该怎么办
19.11 重新获得控制
19.12 找到黑客修改的文件
19.12.1 解释tar -d的输出
19.12.2 用RPM加速检查
19.12.3 RPM修复
19.12.4 恢复数据库
19.12.5 外设损害
19.12.6 通过恶意电子邮件偷窃
19.12.7 内核会被怎样破坏
19.13 封锁攻击
19.14 找到set-UID程序
19.15 找到mstream特洛伊木马
第20章 找出黑客的系统
20.1 用nslookup跟踪数字IP地址
20.2 用dig跟踪数字IP地址
20.3 查找.com拥有者
20.4 从IP地址直接找到黑客
20.5 查找.gov系统
20.6 使用ping
20.7 使用traceroute
20.8 邻近系统的结果
20.9 最近一次对黑客的国际追踪
20.10 确信你找到了攻击者
20.11 其他系统管理员：他们关心吗
第21章 惩罚黑客
21.1 警察会有多大帮助
21.1.1 FBI
21.1.2 美国秘密服务
21.1.3 其他联邦机构
21.1.4 州立机构
21.1.5 本地警察
21.1.6 准备你的案子
21.1.7 跟踪被盗的数据
21.1.8 关心证据
21.2 起诉
21.3 允许非法行为的ISP要负的责任
21.4 反击
21.4.1 法律问题
21.4.2 大量垃圾邮件攻击
21.4.3 死亡性ping
21.4.4 恶意的Java Applet
21.4.5 雇佣打手
第五部分 附 录
附录A 有关安全技术的最新网上资源
附录B 其他参考资源
附录C 网络服务和端口

附录D PORTS.C程序清单
附录E BLOCKIP.CSH程序清单
附录F FPROMISC.CSH程序清单
附录G OVERWRITE.C程序清单
附录H 危险等级
附录I 本书附带光盘的内容
附录J 术语表

版权说明