第一图书网, tushu007.com

<<Linux安全最大化>>

图书基本信息

书名：<<Linux安全最大化>>

13位ISBN编号：9787505372863

10位ISBN编号：7505372866

出版时间：2002-1

出版时间：电子工业出版社

作者：(美)Anonymous等

页数：633

字数：1017

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

第一图书网, tushu007.com

<<Linux安全最大化>>

内容概要

本书详细论述了Linux系统的安全问题。
全书共分五大部分，分别讨论Linux安全基础、Linux用户安全、Linux网络安全、Linux Internet安全命令。
涉及的问题包括物理安全、安装问题、基本Linux系统管理，如何防御口令攻击和数据攻击，恶意代码、嗅探器和电子窃听，扫描仪及电子欺骗的原理和防范措施，各种Internet服务的安全性、防火墙、入侵检测、日志和审计跟踪、灾难恢复等。
本书适合

第一图书网, tushu007.com

<<Linux安全最大化>>

书籍目录

前言第一部分 Linux安全基础第1章 Linux概述1.1 什么是Linux1.1.1 Linux是自由的1.1.2 Linux非常类似于Unix1.1.3 Linux来自哪里1.1.4 为什么Linux不适合所有人1.2 Linux作为独立的系统使用1.3 Linux作为Intranet/Internet服务器1.4 Linux安全概述1.4.1 用户账号1.4.2 自主访问控制1.4.3 网络访问控制1.4.4 加密1.4.5 内置日志、审计和网络监视功能1.4.6 入侵检测1.5 小结第2章 物理安全2.1 服务器的位置和物理访问2.1.1 网络运行中心2.1.2 公共计算实验室2.1.3 计算机使用策略2.2 网络拓扑结构2.2.1 网络拓扑结构分类2.2.2 拓扑结构安全小结2.3 网络硬件2.3.1 常规的网络硬件安全措施2.3.2 网络硬件小结2.4 工作站和安全2.4.1 BIOS和控制台口令2.4.2 生物统计学访问控制2.4.3 调制解调器安全2.4.4 防盗设备2.4.5 惟一数字、标价和其他技术2.5 小结第3章 安装问题3.1 关于不同Linux版本、安全性及安装方法3.1.1 不同Linux版本不尽相同3.2 分区和安全3.2.1 分区究竟是什么3.2.2 把Linux集中安装在单一分区3.2.3 多分区的其他优点3.2.4 分区大小3.2.5 创建交换分区和根分区3.2.6 创建扩展分区3.2.7 在扩展分区中创建逻辑分区3.2.8 其他分区工具3.2.9 分区和安全小结3.3 安装时选择网络服务3.3.1 提高系统安全5分钟3.3.2 chkconfig3.4 引导加载程序3.4.1 ／etc／lilo.conf：LILO配置文件3.4.2 引导装载程序小结3.5 小结第4章 基本Linux系统管理4.1 基本概念4.1.1 你自己的账号4.2 创建和管理账号4.2.1 账号策略4.2.2 账号结构4.2.3 添加用户4.2.4 使用自己的工具添加用户4.2.5 删除用户4.3 使用su执行管理任务4.3.1 su——替代用户4.4 访问控制4.5 访问权限和所有权4.5.1 chmod：更改文件访问权限4.6 进一步了解组4.6.1 创建组4.6.2 chown：设置用户所有者和组访问权限4.6.3 删除组4.7 关闭系统4.7.1 shutdown：关闭Linux系统4.8 小结第二部分 Linux用户安全第5章 口令攻击5.1 什么是口令攻击5.2 Linux如何生成和保存口令5.2.1 口令回顾5.3 数据加密标准5.3.1 字典攻击5.4 案例研究：通过字典攻击来破解Linux口令5.4.1 字典攻击：历史透视5.5 口令隐藏和隐藏套件5.5.1 ／etc／shadow：口令shadow数据库5.5.2 创建和删除用户和组的背后5.5.3 针对隐藏系统的可能的攻击5.6 安装完shadow套件之后5.6.1 口令选择及系统安全5.7 其他口令安全问题5.7.1 口令增殖和安全5.8 嵌入式认证模块5.9 其他口令安全解决方案5.9.1 关于网络信息服务和口令安全5.10 小结第6章 数据攻击6.1 什么时候需要考虑数据安全6.1.1 现实的攻击6.2 数据安全的类型6.2.1 私钥系统6.2.2 公共密钥系统6.3 通用加密算法6.4 mcrypt：安装和使用6.4.1 使用mcrypt6.5 GnuPG：安装和使用公共密钥加密工具6.5.1 生成密钥对6.5.2 使用密钥链6.5.3 加密和解密文档6.5.4 为GnuPG添加GUI6.6 隐藏术——另类加密6.6.1 安装和使用JPHIDE／JPSEEK6.7 其他资源6.8 小结第三部分 Linux网络安全第7章 恶意代码7.1 什么是恶意代码7.1.1 什么是特洛伊7.1.2 病毒7.2 检测恶意代码7.2.1 Tripwire7.2.2 Tripwire的获得7.2.3 安装Tripwire7.2.4 配置和运行Tripwire7.2.5 使用Tripwire检查文件完整性7.2.6 Tripwire小结7.3 其他文件完整性检查软件7.3.1 TAMU7.3.2 Aide7.3.3 ATP（反篡改程序）7.3.4 Distributed L67.3.5 Hobgoblin7.3.6 sXid7.3.7 trojan.pl7.3.8 其他资源7.4 小结第8章 嗅探器和电子窃听8.1 嗅探器工作原理8.2 案例分析：执行几个简单的嗅探器攻击8.2.1 linsniffer8.2.2 linux_sniffer8.2.3 hunt8.2.4 sniffit8.3 其他嗅探器和网络监听工具8.4 嗅探器引起的风险8.5 嗅探器攻击的防范8.5.1 ifconfig8.5.2 NEPED：Ethernet网络混乱模式检测器8.5.3 其他更通用的嗅探器防范工具8.6 更多资料8.7 小结第9章 扫描器9.1 扫描器简介9.1.1 剖析系统扫描器9.1.2 剖析网络扫描器9.2 扫描器构件和扫描器发展9.2.1 SATAN9.3 将扫描器融入安全体系9.4 各种扫描工具9.4.1 SAINT9.4.2 Nessus9.4.3 nmap——网络映射器9.4.4 CGI扫描器v1.09.4.5 扫描器是否合法9.5 防范扫描器攻击9.5.1 courtney（SATAN和SAINT检测器）9.5.2 IcmpInfo（ICMP扫描／炸弹探测器）5.5.3 scan－detector（通用UDP扫描检测器）9.5.4 klaxon9.5.5 Psionic PortSentry9.6 相关资源9.7 小结第10章 电子欺骗10.1 电子欺骗的真正含义10.2 TCP和IP欺骗10.3 案例分析：一个简单的欺骗攻击10.3.1 攻击实例10.3.2 TCP和IP欺骗工具10.3.3 容易遭受IP欺骗的服务10.4 阻止IP欺骗攻击10.5 ARP欺骗10.5.1 阻止ARP欺骗攻击10.6 DNS欺骗10.7 其他古怪的欺骗攻击10.8 Couic10.9 进一步的阅读10.10 小结第四部分 Linux Internet安全第11章 FTP安全11.1 文件传输协议11.1.1 FTP安全历史11.2 FTP默认的安全功能11.2.1 ／etc／ftpusers：受限制的用户访问文件11.2.2 ／etc／ftpcess：ftpd配置文件11.3 SSH文件传输11.3.1 scp11.3.2 sftp11.3.3 替代方案：SSLftp和sftp11.4 特定的FTP应用程序的安全11.4.1 ncftp11.4.2 filerunner11.4.3 ftpwatch11.4.4 wu－ftpd11.5 小结第12章 邮件安全12.1 SMTP服务器和客户端12.1.1 一个简单的SMTP客户程序12.2 sendmail安全基础12.2.1 sendmail服务保护12.2.2 其他sendmail资源12.3 用Qmail替代sendmail12.3.1 Qmail的安装12.3.2 其他Qmail资源12.4 小结第13章 Telnet和SSH安全13.1 Telnet的安全历

第一图书网, tushu007.com

史13.2 安全telnet系统13.3 deslogin13.3.1 安装deslogin软件包13.3.2 STEL（安全Telnet）13.4 德克萨斯农业与机械大学开发的SRA Telnet13.5 斯坦福SRP Telnet／FTP软件包13.5.1 重要文档13.6 Secure Shell13.6.1 ssh核心工具13.6.2 快速安装ssh软件包13.6.3 ssh服务器配置13.6.4 sshd启动命令行选项13.6.5 启动sshd13.6.6 使用ssh客户程序13.7 scp：安全拷贝远程文件拷贝程序13.8 为多操作系统网络提供ssh服务13.8.1 PuTTY13.8.2 Tera Term13.8.3 Macintosh下的ssh支持13.8.4 运行中的ssh实例13.9 ssh安全问题13.10 更多资料13.11 小结第14章 Web服务器安全14.1 删除不必要的服务14.1.1 文件传输协议（FTP）14.1.2 finger14.1.3 网络文件系统（NFS）14.1.4 其他RPC服务14.1.5 rwalld（rwall服务器）14.1.6 R服务14.1.7 其他服务14.1.8 对运行服务实施访问控制14.2 Web服务器安全14.2.1 httpd14.2.2 控制外部访问：httpd.conf14.2.3 影响安全的配置选项14.2.4 ExecCGI选项：允许CGI程序运行14.2.5 FollowSymLinks选项：允许用户跟随符号链接浏览14.2.6 Includes选项：激活服务器端嵌入（SSI）14.2.7 Indexes选项：激活目录索引14.3 使用基本的HTTP认证添加目录访问控制14.3.1 htpasswd14.4 基本HTTP认证的弱点14.5 HTTP和加密认证14.5.1 添加MD5摘要认证14.6 运行chroot Web环境14.7 WebDAV14.7.1 安装和配置WebDAV14.7.2 在Mac OS X下使用WebDAV14.7.3 在Windows下使用WebDAV14.8 授权和认证14.8.1 PricewaterhouseCoopers，Resource Protection Services（USA）14.8.2 美国合格公共会计师协会（AICPA）14.8.3 国际计算机安全协会（ICSA，其前身为NCSA）14.8.4 Troy Systems14.9 小结第15章 安全Web协议15.1 问题15.2 Netscape Communications公司开发的安全套接字层（SSL）15.2.1 SSL的安全历史15.3 安装mod_ssl15.3.1 解压、编译和安装OpenSSL15.3.2 解压、编译和安装mod_ssl15.3.3 测试服务器IS.3.4 关于证书和证书管理机构15.3.5 Apache－SSL小结15.3.6 SSL的进一步阅读资料15.4 小结第16章 安全Web开发16.1 开发风险因素概论16.2 生成Shell16.2.1 使用system（）执行Shell命令16.2.2 C和C＋＋中的popen（）16.2.3 Perl中的open（）16.2.4 eval（Perl和shell）16.2.5 Perl中的exec（）16.3 缓冲溢出（Buffer Overrun）16.3.1 关于通常的用户输入16.4 路径、目录和文件16.4.1 chdir（）16.4.2 文件16.5 嵌入式编程语言16.5.1 安装PHP16.5.2 其他嵌入式语言16.6 自动化CGI测试工具16.6.1 其他值得关注的安全编程和测试工具16.7 其他在线资源16.8 小结第17章 文件共享安全17.1 Linux作为文件服务器17.2 Samba17.2.1 全局安全指令17.2.2 共享级别指令17.2.3 SWAT17.2.4 其他资源17.3 Netatalk17.3.1 基本Netatalk配置17.3.2 更多信息17.4 NFS安全17.4.1 exports17.4.2 其他参考资料17.5 虚拟专用网17.5.1 IPSEC17.6 小结第18章 拒绝服务攻击18.1 什么是拒绝服务攻击18.2 拒绝服务攻击带来的危险18.2.1 分布式拒绝服务攻击（DDoS）18.3 本章的组织结构18.4 网络硬件DoS攻击18.5 针对Linux网络的攻击18.5.1 knfsd攻击18.5.2 ICMP分段攻击18.5.3 sesquipedalian.c18.5.4 inetd和NMAP18.5.5 lpd伪造打印请求18.5.6 mimeflood.pl18.5.7 portmap（以及其他RPC服务）18.5.8 Unix Socket垃圾收集DoS18.5.9 time和daytime DoS18.5.10 teardrop.c18.5.11 identd打开的套接字泛洪18.5.12 Lynx／chargen浏览器攻击18.5.13 nestea.c18.5.14 pong.c和ICMP泛洪18.5.15 Ping of Death18.5.16 octopus.c18.6 针对Linux应用程序的攻击18.6.1 Netscape Communicator内容类型（1）18.6.2 Netscape Communicator内容类型（2）18.6.3 passwd资源枯竭18.6.4 xdm18.6.5 wtmp锁18.7 其他DoS攻击18.8 防范拒绝服务攻击18.9 在线资源18.10 小结第19章 Linux和防火墙19.1 什么是防火墙19.1.1 网络级防火墙：数据包过滤器19.1.2 应用程序－代理防火墙/应用程序网关19.2 评估是否真正需要防火墙19.3 Internet网关／防火墙19.4 tcpd：TCP Wrappers19.4.1 TCP Wrappers和网络访问控制19.4.2 TCP Wrappers小结19.5 ipfwadm19.5.1 ipfwadm基础19.5.2 配置ifwadm19.6 ipchains19.6.1 ipchains的安全历史19.7 iptables19.8 Linux下的免费防火墙工具和附件19.9 商业防火墙19.9.1 CSM Proxy/企业版19.9.2 GNAT Box Firewall19.9.3 NetScreen19.9.4 Sun Cobalt Adaptive Firewall19.9.5 PIX Firewal19.10 其他资源19.11 小结第20章 入侵检测20.1 什么是入侵检测20.2 入侵检测基本概念20.3 一些值得关注的入侵检测工具20.3.1 chkwtmp20.3.2 tcplogd20.3.3 Snort20.3.4 HostSentry20.3.5 Shadow20.3.6 MOM20.3.7 蜂鸟系统20.3.8 AAFID20.4 实用入侵检测20.4.1 PortSentry20.4.2 安装并配置PortSentry20.4.3 自动启动20.4.4 入侵检测文档20.5 小结第21章 日志和审计跟踪21.1 日志究竟是什么21.2 Linux日志21.2.1 lastlog21.2.2 last21.2.3 xferlog21.2.4 httpd日志21.2.5 Samba21.2.6 系统和内核消息21.2.7 /Var/log/messages：记录系统和内核消息21.2.8 从自己的程序写入syslog21.2.9 备份和处理日志21.3 其他值得关注的日志和审计工具21.3.1 SWATCH（系统监视器）21.3.2 SNORT21.3.3 Watcher21.3.4 NOCOL/NetConsole v4.021.3.5 PingLogger21.3.6 LogSurfer21.3.7 Netlog21.3.8 Analog21.4 小结第22章 灾难恢复22.1 什么是灾难恢复22.1.1 为什么需要灾难恢复计划22.2 在建立Linux网络前应采取的步骤22.2.1 硬件标准化22.2.2 软件标准化：基

第一图书网, tushu007.com

<<Linux安全最大化>>

本配置22.3 选择备份工具22.4 简单归档：tar、Zip文件和目录22.4.1 创建tar档案文件22.4.2 使用gzip压缩tar档案文件22.4.3 kArchiver22.4.4 cpio：另一个文件档案工具22.4.5 创建“ 热 ”档案站点22.5 备份类型和备份策略22.6 备份软件包22.6.1 KDat22.6.2 KBackup（由Karsten开发）22.6.3 Enhanced Software Technologies的BRU22.6.4 AMANDA（高级马里兰自动网络磁盘归档器）22.7 其他22.8 小结第五部分 附录附录A Linux安全命令参考附录B Linux安全索引——已往的Linux安全问题附录C 其他有用的Linux安全工具附录D 更多的信息来源附录E 术语表

第一图书网, tushu007.com

<<Linux安全最大化>>

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