第一图书网, tushu007.com

<<Linux安全技术内幕>>

图书基本信息

书名：<<Linux安全技术内幕>>

13位ISBN编号：9787302223146

10位ISBN编号：7302223149

出版时间：2010-7

出版时间：清华大学

作者：李洋

页数：626

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

前言

随着黑客攻击问题的不断加剧，木马、病毒、网络钓鱼、分布式拒绝服务攻击、僵尸网络等网络威胁的不断涌现，信息安全问题已经成为国家、社会和企业关注的焦点问题。
信息安全问题的范围已经扩展到计算机和通信领域的方方面面，其中作为基础软件的操作系统也不例外。
作为一种优秀的开源网络操作系统，Linux在网络技术日益发展的今天，凭借其在安全性、稳定性等方面的巨大优势，正受到越来越多用户的青睐，一些大型网络及网站服务器都建立在Linux平台之上。
然而，其在系统管理、网络服务管理等方面的安全问题仍然不可小视，针对该系统安全问题的分析和相应的安全技术保障已成为广大网络和系统管理员以及众多操作系统用户的迫切需求。
本书从黑客攻击的基本技术、Linux面临的安全威胁、Linux安装与启动、Linux系统安全管理、Linux网络服务安全管理、Linux核心安全技术、Linux优秀开源安全工具等多个层面，力求系统、全面、科学地讲述和揭示与Linux相关的原理、技术、机制等安全内幕。
本书所讲述的Linux安全内容覆盖范围广，适用人群广。
在写作思路上强调在“授人以渔”的前提下“授人以鱼”，对每个知识点的介绍争取做到深入浅出，从系统、科学的原理和机制介绍出发，并通过丰富多样的图表配以具体的步骤实现和详细的讲解。
并且，编者精心选择了目前市面上最为流行和稳定的Fedora 10 Linux操作系统版本进行实例讲解，以方便读者在实际L,inux安全的管理和操作中进行对照学习，提高学习效率。

第一图书网, tushu007.com

<<Linux安全技术内幕>>

内容概要

本书系统、全面、科学地讲述和揭示了与Linux相关的原理、技术、机制等安全内幕，全书共分25章，对Linux安全内幕进行了全面、深入，和系统的分析，内容包括黑客攻击的基本技术、Linux面临的安全威胁、Linux安装与启动、Linux系统安全管理、Linux网络服务安全管理、Linux核心安全技术、Linux优秀开源安全工具等。

本书的讲解和分析深入透彻，适用于众多Linux爱好者、中高级Linux用户、IT培训人员及IT从业者，同时也兼顾网络管理员和信息安全工作者，并可作为高等院校计算机和信息安全专业学生的教学参考书。

第一图书网, tushu007.com

作者简介

李洋，博士，信息安全专家，项目经理。
10余年来一直从事计算机网络信息安全领域研发工作，曾主持和参与多项国家重点项目以及信息安全系统和企业信息安全系统的研发工作。
在IEEE、ACM、《计算机世界》、《网管员世界》、51CTo等国际和国内知名会议、期刊和媒体上发表学术论文和各类技术文章百余篇，并出版相关专著多部。

第一图书网, tushu007.com

<<Linux安全技术内幕>>

书籍目录

第1章 Linux安全基础 1.1 信息安全的重要性 1.1.1 网络信息安全的基本概念 1.1.2 网络威胁的基本表现 1.1.3 网络信息安全领域的研究重点 1.1.4 网络信息安全的五要素 1.1.5 经典的P2DR模型 1.2 黑客攻击的常见手段和步骤 1.2.1 黑客攻击的常见方法 1.2.2 黑客攻击的一般步骤 1.3 Linux操作系统的安全性 1.3.1 Linux操作系统的安全级别 1.3.2 现行Linux操作系统的安全机制 1.4 Linux网络安全基础 1.4.1 网络基本原理 1.4.2 TCP/IP网络 1.4.3 IP协议 1.4.4 TCP协议 1.4.5 UDP协议 1.4.6 ARP和RARP协议 1.4.7 ICMP协议 1.4.8 IPv4和IPv6 1.5 国内外相关安全标准概述第2章 Linux概述 2.1 Linux的历史 2.2 与Linux相关的基本概念 2.2.1 开源软件 2.2.2 GNU 2.2.3 GPL 2.2.4 POSIX 2.3 Linux的主要特点 2.4 Linux的应用领域 2.5 Linux的内核及发行版本 2.6 常见的Linux发行版本 2.6.1 Red Hat Linux 2.6.2 Fedora Core/Fedora 2.6.3 Debian 2.6.4 Ubuntu 2.6.5 SuSE Linux 2.6.6 Mandriva 2.7 Linux的主要组成部分 2.7.1 内核 2.7.2 Shell 2.7.3 文件结构 2.7.4 实用工具 2.8 Fedora Linux的发展历史 2.9 Fedora的主要特征第3章 Fedora 10的安全安装与启动 3.1 Fedora 10的安装 3.1.1 硬件需求 3.1.2 安装方式 3.1.3 安装过程 3.2 Fedora 10的启动与登录 3.2.1 安全登录Linux 3.2.2 退出Linux 3.3 Linux的启动安全 3.3.1 Linux的启动过程 3.3.2 Linux的运行级别 3.3.3 GRUB密码设定第4章 用户和组安全 4.1 用户和组管理的基本概念 4.2 安全使用用户和组文件 4.2.1 用户账号文件——passwd 4.2.2 用户影子文件——shadow 4.2.3 组账号文件——group 4.2.4 组账号文件——gshadow 4.2.5 /etc/skel目录 4.2.6 /etc/login.defs 配置文件 4.2.7 /etc/default/useradd文件 4.3 安全管理用户和组工具 4.3.1 useradd：添加用户工具 4.3.2 usermod：修改用户信息工具 4.3.3 userdel：删除用户工具 4.3.4 groupadd：创建组工具 4.3.5 groupmod：修改组属性工具 4.3.6 groupdel：删除组工具 4.3.7 其他工具 4.4 使用Fedora用户管理器管理用户和组 4.4.1 启动Fedora用户管理器 4.4.2 创建用户 4.4.4 创建用户组 4.4.5 修改用户组属性 4.5 与用户和组管理安全相关的其他安全机制 4.5.1 验证用户和组文件 4.5.2 用户密码的安全设定方法 第5章 保证Linux文件系统安全 5.1 Linux文件系统原理 5.1.1 Linux中的文件系统类型 5.1.2 Linux文件的类型 5.1.3 Linux中的目录结构设定 5.2 安全设定文件/目录访问权限 5.02.1 文件/目录访问权限基本概念 5.2.2 改变文件/目录的访问权限 5.2.03 更改文件/目录的所有权 5.2.4 改变文件的执行权限 5.3 使用额外属性保护Ext3文件系统安全 5.3.1 Ext3中的额外属性 5.3.2 使用Ext3文件系统的属性 5.3.3 Ext3属性和文件权限的区别 5.3.4 使用chattr 5.4 使用加密文件系统 5.04.1 内核准备 5.4.2 创建加密设备 5.4.3 卸载加密设备 5.4.4 重新装载加密设备 5.4.5 在Linux系统安装时使用EFS 第6章 Linux系统安全增强技术 6.1 Linux安全增强的经典模型 6.1.1 BLP安全模型 6.1.2 基于角色的访问控制模型 6.1.3 多级别安全机制 6.1.4 操作系统安全加固方法 6.2 SELinux：Linux安全增强机制 6.2.1 SELinux的历史 6.2.2 SELinux基本原理 6.2.3 SELinux相对于传统机制的优势 6.2.4 SELinux中的上下文 6.2.5 SELinux中的目标策略 6.2.6 使用SELinux配置文件和策略目录 6.2.7 使用SELinux的先决条件 6.2.8 SELinux中的布尔变量第7章 Linux进程安全 7.1 Linux进程的基本原理 7.1.1 进程类型 7.1.2 进程的状态 7.1.3 进程的工作模式 7.1.4 进程与线程的区别 7.2 Linux下的守护进程 7.2.1 守护进程基本原理 7.2.2 Linux下的重要守护进程 7.3 安全管理Linux进程 7.手工启动Linux进程 7.3.2 自动执行进程 7.3.3 资源空闲时执行进程 7.3.4 周期性执行进程 7.3.5 操作cron后台进程 7.3.6 挂起及恢复进程 7.4 查看及终止进程 7.4.1 使用ps命令查看进程状态 7.4.2 使用top命令查看进程状态 7.4.3 使用kill命令终止进程 7.4.4 使用sleep命令暂停进程 7.5 安全管理每个进程的系统资源 7.5.1 限制进程创建大型文件 7.5.2 限制单个用户调用的最大子进程个数 7.6 进程文件系统PROC 第8章 Linux日志管理安全 8.1 Linux日志管理简介 8.2 Linux下重要日志文件介绍 8.2.1 /var/log/boot.log 8.2.2 /var/log/cron 8.2.3 /var/log/maillog 8.2.4 /var/log/syslog 8.2.5 /var/log/wtmp 8.2.6

第一图书网, tushu007.com

/var/run/utmp 8.2.7 /var/log/xferlog 8.3 Linux下基本日志管理机制 8.3.1 who命令 8.3.2 users命令 8.3.3 last命令 8.3.4 ac命令 8.3.5 lastlog命令 8.4 使用syslog设备 8.4.1 syslog简介 8.4.2 syslog配置文件 8.4.03 syslog进程 8.5 Linux日志使用的重要原则 8.6 Linux日志输出查看方式 8.6.1 dmesg 8.6.2 tail 8.6.3 more和less 8.6.4 其他式 第9章 xinetd安全管理Linux网络服务 9.1 xinetd原理 9.2 xinetd服务配置文件 9.3 通过文件配置使用xinetd 9.4 通过图形用户界面进行配置使用xinetd 第10章 DHCP服务安全 10.1 DHCP原理 10.1.1 DHCP简介 10.1.2 DHCP的工作流程 10.2 安装和启动DHCP服务器 10.2.1 安装DHCP服务器 10.2.2 启动和关闭DHCP服务器 10.3 安全配置DHCP服务 10.3.1 DHCP服务器配置文件 10.3.2 DHCP服务器配置实例 10.3.3 指定DHCP为指定网卡服务 10.4 安全配置DHCP客户端 10.4.1 图形界面配置Linux客户端 10.4.2 配置文件配置Linux客户端 10.5 使用chroot保证DHCP运行安全 10.5.1 下载和安装Jail软件 10.5.2 使用Jail创建chroot牢笼 第11章 DNS服务安全 11.1 DNS域名服务原理简介 11.1.1 DNS简介 11.1.2 DNS系组成及基本概念 11.1.3 DNS服务器的类型 11.1.4 DNS的工作原理 11.2 安装和启动DNS服务器 11.2.1 安装DNS服务器 11.2.2 启动和关闭DNS服务器 11.3 安全配置DNS服务器 11.3.1 DNS服务器配置文件类型 11.3.2 named.conf主配置文件 11.3.3 区文件 11.3.4 DNS服务器配置实例 11.3.5 安全配置DNS客户端 11.4 安全使用DNS服务器的高级技巧 11.4.1 配置辅助域名服务器做到冗余备份 11.4.2 配置高速缓存服务器提高DNS服务器性能 11.4.3 配置DNS负载均衡防止服务器宕机 11.4.4 配置智能DNS高速解析 11.4.5 合理配置DNS的查询方式提高效率 11.4.6 使用dnstop监控DNS流量 11.4.7 使用DNSSEC技术保护DNS安全 第12章 邮件服务安全 12.1 邮件系统简介 12.1.1 邮件传递代理（MTA） 12 邮件存储和获取代理（MSA） 12.1.3 邮件客户代理（MUA） 12.2 SMTP介绍 12.2.1 SMTP的模型 12.2.2 SMTP的基本命令 12.3 安装与启动Sendmail 12.4 安全配置sendmail.cf 12.5 安全配置sendmail.mc文件 12.6 防治垃圾邮件 12.6.1 常用技术 12.6.2 配置Sendmail防范垃圾邮件 12.6.3 使用SpamAssasin防治垃圾邮件 第13章 FTP服务安全 13.1 FTP简介 13.1.1 FTP协议介绍 13.1.2 FTP文件类型 13.1.3 FTP文件结构 13.1.4 FTP传模式 13.1.5 FTP常用命令 13.1.6 FTP典型消息 13.2 安装和启动vsftpd服务器 13.2.1 装vsftpd 13.2.2 启动和关闭vsftpd 13.2.3 安全配置ftpusers文件 13.2.4 安全配置user_list文件 13.2.5 安全配置vsftpd.conf文件 13.2.6 配置其他一些安全选项 13.3 安全使用vsftpd服务器 13.3.1 匿名用户使用vsftpd服务器 13.3.2 本地用户使用vsftpd服务器 13.3.3 虚拟用户使用vsftpd服务器 13.3.4 配置vsftpd服务器中chroot 13.3.5 配置vsftpd服务器在非标准端口工作 13.3.6 配置虚拟FTP服务器 13.3.7 使用主机访问控制第14章 Web服务安全 14.1 Web服务器简介 14.1.1 HTTP基本原理 14.1.2 Apache服务器简介 14.2 安装Apache的最新版本 14.3 配置Apache服务器主文件 14.4 使用特定的用户运行Apache服务器 14.5 配置隐藏Apache服务器的版本号 14.6 实现访问控制 14.6.1 访问控制常用配置指令 14.6.2 使用.htaccess文件进行访问控制 14.7 使用认证和授权保护Apache 14.7.1 认证和授权指令 14.7.2 管理认证口令文件和认证组文件 14.7.3 认证和授权使用实例 14.8 设置虚拟目录和目录权限 14.9 使用Apache中的安全模块 14.9.1 Apache服务器中安全相关模块 14.9.2 开启安全模块 14.10 使用SSL保证安全 14.10.1 SSL简介 14.10.2 Apache中运用SSL的基本原理 14.10.3 安装和启动SSL 14.11 Apache日志管理 14.11.1 日志管理概述 14.11.2 日志相关的配置指令 14.11.3 日志记录等级和分类 14.11.4 几个重要的日志文件第15章 代理服务安全 15.1 代理服务器简介 15.2 Squid简介 15.3 安装和启动Squid Server 15.3.1 安装Squid Server 15.3.2 启动和关闭Squid Server 15.4 在客户端使用Squid Server 15.4.1 在IE浏览器设置 15.4.2 在Linux浏览器中设置 15.5 安全配置Squid Server 15.5.1 配置Squid Server的基本参数 15.5.2 配置Squid Server的安全访问控制 15.5.3 配置Squid Server的简单实例 15.6 安全配置基于Squid的透明代理 15.6.1 Linux内核的相关配置 15.6.2 Squid的相关配置选项 15.6.3 iptables的相关配置 15.7 安全配置多级缓存改善Proxy服务器的性能 15.7.1 多级缓存简介 15.7.2 配置多级缓存 15.8 Squid日志管理 15.8.1 配置文件中有关日志的选项 15.8.2 日志管理主文件

第一图书网, tushu007.com

<<Linux安全技术内幕>>

——access.conf 第16章 防火墙技术 16.1 防火墙技术原理 16.1.1 防火墙简介 16.1.2 防火墙的分类 16.1.3 传统防火墙技术 16.1.4 新一代防火墙 16.1.5 防火墙技术的发展趋势 16.1.6 防火墙的配置方式 16.2 Netfilter/iptables防火墙框架 16.2.1 简介 16.2.2 安装和启动Netfilter/iptables系统 16.2.3 iptables基本原理 16.3 iptables简单应用 16.4 使用IPtables完成NAT功能 16.4.1 NAT简介 16.4.2 NAT的原理 16.4.3 NAT具体使用 16.5 防火墙与DMZ 16.5.1 DMZ原理 16.5.2 构建DMZ 第17章 入侵检测技术 17.1 入侵检测系统简介 17.2 入侵检测技术的发展 17.3 入侵检测的分类 17.3.1 入侵检测技术分类 17.3.2 入侵检测系统分类 17.4 Snort简介 17.5 安装Snort 17.6 Snort的工作模式 17.6.1 嗅探器模式 17.6.2 数据包记录器 17.6.3 网络入侵检测模式 17.7 Snort的使用方式 17.7.1 命令简介 17.7.2 查看ICMP数据报文 17.7.3 配置Snort的输出方式 17.7.4 配置Snort规则 17.8 自己动手编写Snort规则 17.8.1 规则动作 17.8.2 协议 17.8.3 IP地址 17.8.4 端口号 17.8.5 方向操作符 17.8.6 activate/dynamic规则 17.8.7 一些重要的指令 17.8.8 一些重要的规则选项 17.8.9 使用Snort检测攻击 17.9 使用Snortcenter构建分布式入侵检测系统 17.9.1 分布式入侵检测系统的构成 17.9.2 系统安装及部署 第18章 Linux集群技术 18.1 集群技术 18.1.1 集群简介 18.1.2 集群系统的分类 18.1.3 高可用集群 18.1.4 高性能计算集群 18.2 Linux中的集群 18.2.1 Linux集群分类 18.2.2 科学集群 18.2.3 负载均衡集群 18.2.4 高可用性集群 18.3 LVS 18.3.1 LVS原理 18.3.2 安装LVS 18.3.3 配置使用LVS第19章 VPN技术 19.1 VPN技术原理 19.1.1 VPN简介 19.1.2 VPN的分类 19.2 Linux下的VPN 19.2.1 IPSec VPN 19.2.2 PPP Over SSH 19.2.3 CIPE：Crypto IP Encapsulation 19.2.4 SSL VPN 19.2.5 PPTP 19.3 使用OpenVPN 19.3.1 OpenVPN简介 19.3.2 安装OpenVPN 19.3.3 制作证书 19.3.4 配置服务端 19.3.5 配置客户端 19.3.6 配置实例 第20章 Samba共享服务安全 20.1 Samba服务简介 20.1.1 Samba工作原理 20.1.2 Samba服务器的功能 20.1.3 SMB协议 20.1.4 Samba服务的工作流程 20.2 安装和启动Samba 20.3 安全配置Samba服务器的用户信息 20.3.1 创建服务器待认证用户 20.3.2 将用户信息转换为Samba用户信息 20.3.3 用户转换 20.3.4 Samba服务器和主浏览器 20.4 smb.conf文件配置详解 20.4.1 设置工作组 20.4.2 设置共享Linux账户主目录 20.4.3 设置公用共享目录 20.4.4 设置一般共享目录 20.4.5 设置共享打印机 20.4.6 具体设置实例 20.5 smb.conf中的选项和特定约定 20.6 使用testparm命令测试Samba服务器的配置安全 20.7 使用Samba日志 20.8 Linux和Windows文件互访 20.8.1 Windows客户使用Linux系统共享文件 20.8.2 用smbclient工具访问局域网上的Windows系统 20.8.3 用smbclient工具访问局域网上的其他系统 第21章 网络文件系统安全 21.1 NFS服务概述 21.1.1 NFS基本原理 21.1.2 NFS服中的进程 21.2 安装和启动NFS 21.2.1 安装NFS 21.2.2 启动NFS 21.3 NFS安全配置和使用 21.3.1 配置NFS服务器 21.3.2 配置NFS客户机 21.3.3 安全使用NFS服务 21.4 图界面安全配置NFS服务器 21.5 保证NFS安全的使用原则第22章 PGP安全加密技术 22.1 PGP技术原理 22.1.1 PGP简介 22.1.2 PGP原理 22.2 使用GnuPG 22.2.1 GnuPG简介 22.2.2 安装GnuPG 22.2.3 GnuPG的基本命令 22.2.4 详细使用方法 22.2.5 GnuPG使用实例 22.2.6 相关注意事项 第23章 PAM安全认证技术 23.1 PAM认证机制简介 23.2 Linux-PAM的分层体系结构 23.2.1 分层体系结构概述 23.2.2 模块层 23.2.3 应用接口层 23.3 Linux-PAM的配置 23.3.1 Linux-PAM单一配置文件的语法 23.3.2 口令映射机制 23.3.3 基于目录的配置形式 23.4 Linux中常用的PAM安全模块 23.5 Linux-PAM使用举例 23.5.1 使用Linux-PAM控制用户安全登录 23.5.2 使用Linux-PAM控制Samba用户的共享登录 23.5.3 使用Linux-PAM控制FTP用户的登录 第24章 Linux面临的网络威胁及策略 24.1 扫描攻击 24.2 木马 24.3 拒绝服务攻击和分布式拒绝服务攻击 24.3.1 DoS攻击 24.3.2 DDoS攻击 24.4 毒 24.4.1 Linux病毒的起源和历程 24.4.2 病毒的主要类型 24.5 IP Spoofing 24.6 ARP Spoofing 24.7 Phishing 24.8 Botnet 24.9 跨站脚本攻击 24.10 零日攻击 24.11“社会工程”攻击 24.12 使用备份应对网络威胁 24.12.1 一些简单实用的备份命令 24.12.2 备份机制和备份策略 第25章 Linux下优秀的开源安全工具 25.1 Tripwire：系统完整性检查工具 25.1.1

第一图书网, tushu007.com

文件完整性检查的必要性 25.1.2 Tripwire简介 25.1.3 Tripwire的基本工作原理 25.1.4 安装Tripwire 25.1.5 配置Tripwire 25.1.6 使用Tripwire进行文件监控 25.1.7 使用Tripwire的原则和注意事项 25.2 John the Ripper：密码分析及检验工具 25.2.1 John the Ripper简介 25.2.2 安装John the Ripper 25.2.3 基本命令和实用工具 25.2.4 密码分析及检验 25.3 dmidecode：硬件状态监控工具 25.3.1 dmidecode简介 25.3.2 安装dmidecode工具 25.3.3 监控硬件状态 25.4 NMAP：端口扫描工具 25.4.1 NMAP简介 25.4.2 安装NMAP 25.4.3 使用NMAP进行多种扫描 25.5 Wireshark：网络流量捕获工具 25.5.1 Wireshark简介 25.5.2 使用Wireshark 25.6 NTOP：网络流量分析工具 25.6.1 NTOP简介 25.6.2 使用NTOP 25.7 其他工具 25.7.1 安全备份工具 25.7.2 Nessus：网络风险评估工具 25.7.3 Sudo：系统管理工具 25.7.4 NetCat：网络安全界的瑞士军刀 25.7.5 LSOF：隐蔽文件发现工具 25.7.6 Traceroute：路由追踪工具 25.7.7 XProbe：操作系统识别工具 25.7.8 SATAN：系统弱点发现工具 附录A Fedora 10命令参考 附录B VMWare虚拟机安装指南

第一图书网, tushu007.com

章节摘录

插图：由上述介绍可知，Linux操作系统的安全级别仅为C2级，安全级不高，很重要的一个原因就是超级用户具有所有特权，而普通用户不具有任何特权。
操作系统的这种特权管理机制便于系统的维护和配置，但是不利于保证系统的安全性。
一方面，一旦超级用户的口令丢失或者口令让不法用户获取，那么将会对系统造成极大的损失；另一方面，超级用户的误操作以及权限的滥用也对系统的安全构成了极大的威胁。
因此，必须针对该操作系统实行最小特权管理机制。
最小特权管理的主要思想比当前Linux系统的机制更为安全，它指的是系统不赋予用户超过执行任务所需特权之外的特权，也就是说，不存在具有所有权限的用户。
例如，可以将超级用户的特权划分为一组细粒度的特权，分别授予不同的系统管理员或者是相关的操作人员，使得系统中的这些人员只能够使用自己的特权完成相应的属于自己的工作，从而减少了由于特权用户的口令丢失或者是误操作所引起的不必要的损失。
并且，为了保证系统的安全性，不应当将特权集于某个用户，且对其赋予一个以上的职责，这样，就不会由于一权独揽造成权限滥用的不良后果。
当然，根据实际的应用，还是可以按情况对某个用户的权限进行必要的改变和增加，但是在执行这种变化时必须充分考虑到这些改变和权限的增加对系统安全性造成的影响，因此，可以在具体的设计过程中根据实际应用情况进行分别细致的考虑。

第一图书网, tushu007.com

编辑推荐

《Linux安全技术内幕》是由清华大学出版社出版的。

第一图书网, tushu007.com

<<Linux安全技术内幕>>

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