第一图书网, tushu007.com

<<防线：企业Linux安全运维理念 >

图书基本信息

书名：<<防线：企业Linux安全运维理念和实战>>

13位ISBN编号：9787302318071

10位ISBN编号：7302318077

出版时间：2013-8-1

出版时间：清华大学出版社

作者：李洋

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

内容概要

本书作者有多年的世界500强企业的信息安全管理工作经验，深谙500强企业信息安全建设、规划、实施和管理的细节、难点和重点问题。
世界500强企业对于信息安全工作的重视程度，对于信息安全在建设、规划、实施和管理等方面都有其独到之处，可以为其他中小型和大型企业所借鉴和参照。
基于这个目的，本书以笔者在500强企业中使用企业级开源操作系统Linux在信息安全中的部署和使用方法为切入点，来介绍如何做好信息安全工作。

本书共分为5篇，包含19章和两个附录。
面向企业实际需求，对如何使用企业开源Linux操作系统来进行信息安全建设进行了全面、深入和系统的分析，并通过大量的威胁分析、解决思路、解决技术及实现实例来进行介绍。

本书覆盖知识面广，立意较高，几乎覆盖了企业应用开源Linux系统进行信息安全建设的方方面面。

本书适用于信息安全从业人员、众多Linux爱好者、IT培训人员及IT从业者、企业高级管理人员（CIO、CEO、CSO等），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用书。

作者简介

李洋博士，现任某信息安全公司CTO，历任金融公司信息安全顾问、电信运营商和互联网企业信息安全研究员/项目经理。

十余年来一直从事信息安全和IT架构领域的技术研发和管理工作，曾主持和参与多项国家重点项目，并主导多个电信网络、互联网网络、金融企业网络的IT架构设计、信息安全系统设计和研发工作。

具有丰富的企业信息安全规划、架构设计、建设和管理经验，擅长企业信息安全解决方案提供及实施、IT架构设计、网络和系统应用/管理/安全及操作系统内核的研发。

曾在IEEE、ACM、51CTO、《计算机世界》、《网管员世界》等国内外知名媒体和期刊上发表SCI/EI学术论文和各类技术文章百余篇，拥有个人专著6部，国家专利4项。

书籍目录

第一篇 安全运维理论及背景准备
第1章 知彼：企业信息安全现状剖析
1.1 信息安全问题概览
1.1.1 黑客入侵
1.1.2 病毒发展趋势
1.1.3 内部威胁
1.1.4 自然灾害
1.2 各经济大国安全问题概要
1.3 企业面临的主要信息安全威胁
1.3.1 扫描
1.3.2 特洛伊木马
1.3.3 拒绝服务攻击和分布式拒绝服务攻击
1.3.4 病毒
1.3.5 IP欺骗
1.3.6 ARP欺骗
1.3.7 网络钓鱼
1.3.8 僵尸网络
1.3.9 跨站脚本攻击
1.3.1 0缓冲区溢出攻击
1.3.1 1SQL注入攻击
1.3.1 3“ 社会工程学 ”攻击
1.3.1 4中间人攻击
1.3.1 5密码攻击
1.4 认识黑客
1.5 剖析黑客的攻击手段
1.5.1 确定攻击目标
1.5.2 踩点和信息搜集
1.5.3 获得权限
1.5.4 权限提升
1.5.5 攻击实施
1.5.6 留取后门程序
1.5.7 掩盖入侵痕迹
第2章 知己：企业信息安全技术概览
2.1 物理层防护：物理隔离
2.2 系统层防护：安全操作系统和数据库安全
2.2.1 选用安全操作系统
2.2.2 操作系统密码设定
2.2.3 数据库安全技术
2.3 网络层防护：防火墙
2.3.1 防火墙简介
2.3.2 防火墙的分类
2.3.3 传统防火墙技术
2.3.4 新一代防火墙的技术特点
2.3.5 防火墙技术的发展趋势
2.3.6 防火墙的配置方式

2.3.7 防火墙的实际安全部署建议
2.4 应用层防护：IDS/IPS
2.4.1 入侵检测系统简介
2.4.2 入侵检测技术的发展
2.4.3 入侵检测技术的分类
2.4.4 入侵检测系统的分类
2.4.5 入侵防御系统（IPS）
2.4.6 IPS的发展
2.4.7 IPS的技术特征
2.4.8 IPS的功能特点
2.4.9 IPS的产品种类
2.5 网关级防护：UTM
2.6 Web应用综合防护：WAF
2.7 数据防护：数据加密及备份
2.7.1 加密技术的基本概念
2.7.2 加密系统的分类
2.7.3 常用的加密算法
2.7.4 加密算法的主要应用场景
2.7.5 数据备份及恢复技术
2.8 远程访问安全保障：VPN
2.8.1 VPN简介
2.8.2 VPN的分类742.9 身份认证技术
2.9.1 静态密码
2.9.2 智能卡（IC卡）
2.9.3 短信密码
2.9.4 动态口令牌
2.9.5 USBKey
2.9.6 生物识别技术
2.9.7 双因素身份认证
2.1 0管理层：信息安全标准化组织及标准
2.1 0.1 国际信息安全标准概览
2.1 0.2 国内信息安全标准概览
第二篇 企业Linux安全运维规划及选型
第3章 规划：企业信息安全
工作思路
3.1 信息安全的本质
3.2 信息安全概念经纬线：从层次到属性
3.3 业界信息安全专家定义的信息安全：信息安全四要素
3.4 企业信息安全的实施内容和依据（框架）
3.4.1 基本原则
3.4.2 传统的企业信息安全架构
3.4.3 新的企业信息安全框架及其实施内涵
3.5 规划企业Linux安全的实施内容
第4章 选型：企业Linux软硬件选型及安装部署
4.1 Linux应用套件选择
4.1.1 Linux的历史
4.1.2 与Linux相关的基本概念

4.1.3 Linux的主要特点
4.1.4 Linux的应用领域
4.1.5 常见的Linux发行套件
4.1.6 企业的选择：FedoravsRedHatEnterpriseLinux
4.2 Linux内核版本选择
4.3 Linux服务器选型
4.3.1 CPU（处理器）
4.3.2 RAM（内存）
4.3.3 处理器架构
4.3.4 服务器类型选型
4.4 Linux安装及部署
4.4.1 注意事项
4.4.2 其他需求
4.5 大规模自动部署安装Linux
4.5.1 PXE技术
4.5.2 搭建Yum源1174.5.3 安装相关服务
第三篇 企业Linux安全运维实战
第5章 高屋建瓴：“ 四步 ”完成企业Linux系统安全防护
5.1 分析：企业Linux系统安全威胁
5.2 理念：企业级Linux系统安全立体式防范体系
5.3 企业Linux文件系统安全防护
5.3.1 企业Linux文件系统的重要文件及目录
5.3.2 文件/目录访问权限
5.3.3 字母文件权限设定法
5.3.4 数字文件权限设定法
5.3.5 特殊访问模式及粘贴位的设定法
5.3.6 使用文件系统一致性检查工具：Tripwire
5.3.7 根用户安全管理
5.4 企业Linux进程安全防护
5.4.1 确定Linux下的重要进程
5.4.2 进程安全命令行管理方法
5.4.3 使用进程文件系统管理进程
5.4.4 管理中常用的PROC文件系统调用接口
5.5 企业Linux用户安全管理
5.5.1 管理用户及组文件安全
5.5.2 用户密码管理
5.6 企业Linux日志安全管理
5.6.1 Linux下的日志分类
5.6.2 使用基本命令进行日志管理
5.6.3 使用syslog设备
5.7 应用LIDS进行Linux系统入侵检测
5.7.1 LIDS简介
5.7.2 安装LIDS
5.7.3 配置和使用LIDS
第6章 锦上添花：企业Linux操作系统ACL应用及安全加固
6.1 安全加固必要性分析
6.2 加固第一步：使用ACL进行灵活访问控制

6.2.1 传统的用户-用户组-其他用户（U-G-O）访问控制机制回顾
6.2.2 扩展的访问控制列表（ACL）方式
6.3 加固第二步：使用SELinux强制访问控制
6.3.1 安全模型
6.3.2 SELinux：Linux安全增强机制原理
6.3.3 SELinux中的上下文（context）
6.3.4 SELinux中的目标策略（TargetedPolicy）
6.3.5 SELinux配置文件和策略目录介绍
6.3.6 使用SELinux的准备
6.3.7 SELinux中布尔（boolean）变量的使用
第7章 紧密布控：企业Web服务器安全防护
7.1 Web安全威胁分析及解决思路
7.2 Web服务器选型
7.2.1 HTTP基本原理
7.2.2 为何选择Apache服务器
7.2.3 安装Apache
7.3 安全配置Apache服务器
7.4 Web服务访问控制
7.4.1 访问控制常用配置指令
7.4.2 使用.htaccess文件进行访问控制
7.5 使用认证和授权保护Apache
7.5.1 认证和授权指令
7.5.2 管理认证口令文件和认证组文件
7.5.3 认证和授权使用实例
7.6 使用Apache中的安全模块
7.6.1 Apache服务器中安全相关模块
7.6.2 开启安全模块
7.7 使用SSL保证Web通信安全
7.7.1 SSL简介
7.7.2 Apache中运用SSL的基本原理
7.7.3 使用开源的OpenSSL保护Apache通信安全
7.8 Apache日志管理和统计分析
7.8.1 日志管理概述2567.8.2 与日志相关的配置指令
7.8.3 日志记录等级和分类
7.8.4 使用Webalizer对Apache进行日志统计和分析
7.9 其他有效的安全措施
7.9.1 使用专用的用户运行Apache服务器
7.9.2 配置隐藏Apache服务器的版本号
7.9.3 设置虚拟目录和目录权限
7.9.4 使Web服务运行在“ 监牢 ”中
7.1 0Web系统安全架构防护要点
7.1 0.1 Web系统风险分析
7.1 0.2 方案的原则和思路
7.1 0.3 网络拓扑及要点剖析
第8章 谨小慎微：企业基础网络服务防护
8.1 企业基础网络服务安全风险分析
8.1.1 企业域名服务安全风险分析

8.1.2 企业电子邮件服务安全风险分析
8.2 企业域名服务安全防护
8.2.1 正确配置DNS相关文件
8.2.2 使用Dlint工具进行DNS配置文件检查
8.2.3 使用命令检验DNS功能
8.2.4 配置辅助域名服务器进行冗余备份
8.2.5 配置高速缓存服务器缓解DNS访问压力
8.2.6 配置DNS负载均衡
8.2.7 限制名字服务器递归查询功能
8.2.8 限制区传送（zonetransfer）
8.2.9 限制查询（query）
8.2.10分离DNS（splitDNS）
8.2.11隐藏BIND的版本信息
8.2.12使用非root权限运行BIND
8.2.13删除DNS上不必要的其他服务
8.2.14合理配置DNS的查询方式
8.2.15使用dnstop监控DNS流量
8.3 企业电子邮件服务安全防护
8.3.1 安全使用SendmailServer
8.3.2 安全使用Postfix电子邮件服务器
8.3.3 企业垃圾邮件防护
第9章 未雨绸缪：企业级数据防护
9.1 企业数据防护技术分析
9.2 数据加密技术原理
9.2.1 对称加密、解密
9.2.2 非对称加密、解密
9.2.3 公钥结构的保密通信原理
9.2.4 公钥结构的鉴别通信原理
9.2.5 公钥结构的鉴别+保密通信原理
9.3 应用一：使用GnuPG进行应用数据加密
9.3.1 安装GnuPG
9.3.2 GnuPG的基本命令
9.3.3 GnuPG的详细使用方法
9.3.4 GnuPG使用实例
9.3.5 GnuPG使用中的注意事项
9.4 应用二：使用SSH加密数据传输通道
9.4.1 安装最新版本的OpenSSH
9.4.2 配置OpenSSH
9.4.3 SSH的密钥管理
9.4.4 使用scp命令远程拷贝文件
9.4.5 使用SSH设置“加密通道”
9.5 应用三：使用OpenSSL进行应用层加密
9.6 数据防泄露技术原理及其应用
第10章 通道保障：企业移动通信数据防护
10.1 VPN使用需求分析
10.1.1 VPN简介
10.1.2 VPN安全技术分析

10.2 Linux提供的VPN类型
10.2.1 IPSecVPN
10.2.2 PPPOverSSH
10.2.3 CIPE：CryptoIPEncapsulation
10.2.4 SSLVPN
10.2.5 PPPTD
10.3 使用OpenVPN构建SSLVPN
10.3.1 OpenVPN简介
10.3.2 安装OpenVPN
10.3.3 制作证书
10.3.4 配置服务端
10.3.5 配置客户端
10.3.6 一个具体的配置实例
10.4 使用IPSecVPN
10.4.1 安装ipsec-tools
10.4.2 配置IPSecVPN340第11章 运筹帷幄：企业Linux服务器远程安全管理
11.1 远程控制及管理的基本原理
11.1.1 远程监控与管理原理
11.1.2 远程监控与管理的主要应用范围
11.1.3 远程监控及管理的基本内容
11.2 使用Xmanager3.0实现Linux远程登录管理
11.2.1 配置Xmanager服务器端
11.2.2 配置Xmanager客户端
11.3 使用VNC实现Linux远程管理
11.3.1 VNC简介
11.3.2 启动VNC服务器
11.3.3 使用VNCViewer实现Linux远程管理
11.3.4 使用SSH+VNC实现安全的Linux远程桌面管理
第12章 举重若轻：企业网络流量安全管理
12.1 网络流量管理简介
12.1.1 流量识别
12.1.2 流量统计分析
12.1.3 流量限制
12.1.4 其他方面
12.2 需要管理的常见网络流量35812.3 网络流量捕捉：图形化工具Wireshark
12.3.1 Wireshark简介
12.3.2 层次化的数据包协议分析方法
12.3.3 基于插件技术的协议分析器
12.3.4 安装Wireshark
12.3.5 使用Wireshark
12.4 网络流量捕捉：命令行工具tcpdump
12.4.1 tcpdump简介
12.4.2 安装tcpdump
12.4.3 使用tcpdump
12.5 网络流量分析——NTOP
12.5.1 NTOP介绍
12.5.2 安装NTOP

12.5.3 使用NTOP
12.6 网络流量限制——TC技术
12.6.1 TC（TrafficControl）技术原理
12.6.2 使用LinuxTC进行流量控制实例
12.7 网络流量管理的策略
12.7.1 网络流量管理的目标
12.7.2 网络流量管理的具体策略
第13章 兵来将挡，水来土掩：企业级防火墙部署及应用
13.1 防火墙技术简介
13.2 Netfilter/Iptables防火墙框架技术原理
13.2.1 Linux中的主要防火墙机制演进
13.2.2 Netfilter/Iptables架构简介
13.2.3 Netfilter/Iptables模块化工作架构
13.2.4 安装和启动Netfilter/Iptables系统
13.2.5 使用Iptables编写防火墙规则
13.3 使用Iptables编写规则的简单应用
13.4 使用Iptables完成NAT功能
13.4.1 NAT简介
13.4.2 NAT的原理
13.4.3 NAT的具体使用
13.5 防火墙与DMZ的配合使用
13.5.1 DMZ原理
13.5.2 构建DMZ
13.6 防火墙的实际安全部署建议
13.6.1 方案一：错误的防火墙部署方式
13.6.2 方案二：使用DMZ
13.6.3 方案三：使用DMZ+二路防火墙
13.6.4 方案四：通透式防火墙
第14章 铜墙铁壁：企业立体式入侵检测及防御
14.1 入侵检测技术简介
14.2 网络入侵检测及防御：Snort
14.2.1 安装Snort
14.2.2 配置Snort
14.3 编写Snort规则
14.3.1 规则动作
14.3.2 协议
14.3.3 IP地址
14.3.4 端口号
14.3.5 方向操作符（directionoperator）
14.3.6 activate/dynamic规则
14.3.7 Snort规则简单应用举例
14.3.8 Snort规则高级应用举例
14.4 主机入侵检测及防御：LIDS
14.5 分布式入侵检测：SnortCenter
14.5.1 分布式入侵检测系统的构成
14.5.2 系统安装及部署
第四篇 企业Linux安全监控

第15章 管中窥豹：企业Linux系统及性能监控
15.1 常用的性能监测工具
15.1.1 uptime
15.1.2 dmesg
15.1.3 top
15.1.4 iostat
15.1.5 vmstat
15.1.6 sar
15.1.7 KDESystemGuard
15.1.8 free
15.1.9 Traffic-vis
15.1.1 0pmap
15.1.1 1strace
15.1.1 2ulimit
15.1.1 3mpstat
15.2 CPU监控详解
15.2.1 上下文切换
15.2.2 运行队列
15.2.3 CPU利用率
15.2.4 使用vmstat工具进行监控
15.2.5 使用mpstat工具进行多处理器监控
15.2.6 CPU监控总结
15.3 内存监控详解
15.3.1 VirtualMemory介绍
15.3.2 VirtualMemoryPages
15.3.3 KernelMemoryPaging
15.3.4 kswapd
15.3.5 使用vmstat进行内存监控
15.3.6 内存监控总结
15.4 I/O监控详解
15.4.1 I/O监控介绍
15.4.2 读和写数据——内存页
15.4.3 MajorandMinorPageFaults（主要页错误和次要页错误）
15.4.4 TheFileBufferCache（文件缓存区）
15.4.5 TypeofMemoryPages
15.4.6 WritingDataPagesBacktoDisk
15.4.7 监控I/O
15.4.8 CalculatingIO’sPerSecond（IOPS的计算）
15.4.9 RandomvsSequentialI/O（随机/顺序I/O）
15.4.1 0判断虚拟内存对I/O的影响
15.4.1 1I/O监控总结
第16章 见微知著：企业级Linux网络监控
16.1 Cacti网络监控工具简介
16.2 安装和配置Cacti
16.2.1 安装辅助工具
16.2.2 安装Cacti
16.3 使用Cacti

16.3.1 Cacti界面介绍
16.3.2 创建监测点
16.3.3 查看监测点
16.3.4 为已有Host添加新的监控图
16.3.5 合并多个数据源到一张图上
16.3.6 使用Cacti插件
第17章 他山之石：发现企业网络漏洞
17.1 发现企业网络漏洞的大致思路
17.1.1 基本思路
17.1.2 采用网络安全扫描
17.2 端口扫描
17.2.1 端口扫描技术的基本原理
17.2.2 端口扫描技术的主要种类
17.2.3 快速安装Nmap
17.2.4 使用Nmap确定开放端口
17.3 漏洞扫描
17.3.1 漏洞扫描基本原理
17.3.2 选择：网络漏洞扫描与主机漏洞扫描
17.3.3 高效使用网络漏洞扫描
17.3.4 快速安装Nessus50317.3.5 使用Nessus扫描
第五篇 企业Linux安全运维命令、工具
第18章 终极挑战：企业Linux内核构建
18.1 企业级Linux内核简介
18.2 下载、安装和预备内核源代码
18.2.1 先决条件
18.2.2 下载源代码
18.2.3 安装源代码
18.2.4 预备源代码
18.3 源代码配置和编译Linux内核
18.3.1 标记内核
18.3.2.config：配置内核
18.3.3 定制内核
18.3.4 清理源代码树
18.3.5 复制配置文件
18.3.6 编译内核映像文件和可加载模块
18.3.7 使用可加载内核模块
18.4 安装内核、模块和相关文件
18.5 Linux系统故障处理
18.5.1 修复文件系统
18.5.2 重新安装MBR
18.5.3 当系统无法引导时
18.5.4 挽救已安装的系统
第19章 神兵利器：企业Linux数据备份及安全工具
19.1 安全备份工具52219.1.1 Amanda
19.1.2 BackupPC
19.1.3 Bacula
19.1.4 Xtar

19.1.5 Taper
19.1.6 Arkeia
19.1.7 webCDcreator
19.1.8 GhostforLinux
19.1.9 NeroLINUX
19.1.1 0mkCDrec
19.2 Sudo：系统管理工具
19.3 NetCat：网络安全界的瑞士军刀
19.4 LSOF：隐蔽文件发现工具
19.5 Traceroute：路由追踪工具
19.6 XProbe：操作系统识别工具
19.7 SATAN：系统弱点发现工具
附录A 企业级Linux命令速查指南
A.1 文件系统管理命令
A.2 系统管理命令
A.3 系统设置命令
A.4 磁盘管理及维护命令
A.5 网络命令
附录B 网络工具资源汇总

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