

<<蜕变：从菜鸟到Linux安全专家>>

图书基本信息

书名：<<蜕变：从菜鸟到Linux安全专家>>

13位ISBN编号：9787121144349

10位ISBN编号：7121144344

出版时间：2011-9

出版时间：电子工业出版社

作者：李洋 编著

页数：492

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>

<<蜕变：从菜鸟到Linux安全专家>>

内容概要

本书通过实际故事场景对linux安全技术和应用方法进行了全面、深入和系统的分析。分别从黑客攻击的基本技术、linux面临的安全威胁、linux系统安全管理、linux网络服务安全管理、linux核心安全技术等多个层面，向读者系统、全面、科学地讲述了与linux相关的原理、技术和机制等安全方法。

本书覆盖的知识面广，基本覆盖了linux安全的方方面面。本书适用于广大读者群，包括众多linux安全爱好者、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。本书也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。

<<蜕变：从菜鸟到Linux安全专家>>

作者简介

李洋，博士毕业于中科院计算所，现任中国移动通信研究院研究员、项目经理。自2001年以来一直从事计算机网络信息安全领域的研发工作，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。具有丰富的Linux系统应用、管理、安全及内核的研发经验，擅长网络安全技术、网络协议分析、Linux系统安全技术、Linux系统及网络管理、Linux内核开发等。曾在《计算机世界》、《网管员世界》等国内知名媒体上发表各类技术文章百余篇，并出版《Red Hat Linux 9系统与网络管理教程》一书。

<<蜕变：从菜鸟到Linux安全专家>>

书籍目录

菜鸟前传

第1章 上司训话：网络安全态势分析

1.1 网络安全概述

- 1.1.1 网络安全问题概览
- 1.1.2 国际大气候
- 1.1.3 信息安全标准化组织及标准
- 1.1.4 我国的实际情况

1.2 严峻的网络安全现状

- 1.2.1 黑客入侵
- 1.2.2 病毒发展趋势
- 1.2.3 内部威胁
- 1.2.4 自然灾害

1.3 黑客的攻击手段

1.4 重大网络安全威胁汇总

- 1.4.1 scanning
- 1.4.2 木马
- 1.4.3 拒绝服务攻击和分布式拒绝服务攻击
- 1.4.4 病毒
- 1.4.5 ip spoofing
- 1.4.6 arp spoofing
- 1.4.7 phishing
- 1.4.8 botnet
- 1.4.9 跨站脚本攻击
- 1.4.10 零日攻击 (zero day attack)
- 1.4.11 “社会工程学”攻击

1.5 构建企业安全防范体系（架构）

- 1.5.1 企业安全防范体系（架构）的概念
- 1.5.2 企业安全架构的层次结构及相关安全技术
- 1.5.3 企业安全防范架构设计准则

1.6 总结

第2章 一举两得：发现企业网络漏洞

2.1 正中下怀的任务

- 2.1.1 上司的考验
- 2.1.2 打得啪啪响的如意算盘

2.2 发现企业网络漏洞的大致思路

- 2.2.1 基本思路
- 2.2.2 采用网络安全扫描

2.3 端口扫描

- 2.3.1 端口扫描技术基本原理
- 2.3.2 端口扫描技术的主要种类
- 2.3.3 快速安装nmap
- 2.3.4 使用nmap确定开放端口

2.4 漏洞扫描

- 2.4.1 漏洞扫描基本原理
- 2.4.2 选择：网络漏洞扫描或主机漏洞扫描

<<蜕变：从菜鸟到Linux安全专家>>

- 2.4.3 高效使用网络漏洞扫描
- 2.4.4 快速安装nessus
- 2.4.5 使用nessus扫描
- 2.5 总结
- 第3章 初露锋芒：制定linux系统安全保护方案
 - 3.1 方案的具体思路
 - 3.2 圈定linux下的重要文件
 - 3.3 重要文件的权限设置
 - 3.3.1 确定文件/目录访问权限
 - 3.3.2 字母文件权限设定法
 - 3.3.3 数字文件权限设定法
 - 3.3.4 特殊访问模式及粘贴位的设定法
 - 3.4 使用文件系统检查工具检查文件系统
 - 3.4.1 tripwire工具简介
 - 3.4.2 tripwire的安装和配置
 - 3.4.3 使用tripwire扫描文件系统改变
 - 3.5 保护linux下的进程安全
 - 3.5.1 linux下的重要进程
 - 3.5.2 进程安全管理方法
 - 3.5.3 使用进程文件系统管理进程
 - 3.6 保证linux用户管理安全
 - 3.6.1 用户密码管理
 - 3.6.2 管理用户及组文件安全
 - 3.7 做好linux下的日志管理
 - 3.7.1 linux下的日志分类
 - 3.7.2 linux日志管理的基本命令
 - 3.8 总结
- 第4章 sos:拯救崩溃的企业dns
 - 4.1 事故描述
 - 4.2 dns原理及安全概述
 - 4.2.1 dns简介
 - 4.2.2 dns的组成
 - 4.2.3 dns服务器的类型
 - 4.2.4 dns的工作原理
 - 4.2.5 dns面临的安全威胁
 - 4.3 安装和启动dns服务器
 - 4.3.1 安装dns服务器
 - 4.3.2 启动和关闭dns服务器
 - 4.4 安全配置dns服务器
 - 4.4.1 dns服务器配置文件类型
 - 4.4.2 named.conf主配置文件
 - 4.4.3 区文件
 - 4.4.4 dns服务器配置实例
 - 4.4.5 安全配置dns客户端
 - 4.5 安全使用dns服务器的高级技巧
 - 4.5.1 配置辅助域名服务器
 - 4.5.2 配置高速缓存服务器

<<蜕变：从菜鸟到Linux安全专家>>

- 4.5.3 配置dns负载均衡
- 4.5.4 配置智能dns高速解析
- 4.5.5 合理配置dns的查询方式
- 4.5.6 使用dnstop监控dns流量
- 4.5.7 使用dnssec技术保护dns安全
- 4.6 总结
- 第5章 抢班夺权：搞定web服务器管理权限
 - 5.1 web服务器安全防护大赛
 - 5.2 web安全构建方案之web服务器选型
 - 5.2.1 http基本原理
 - 5.2.2 为何选择apache服务器
 - 5.2.3 安装apache
 - 5.3 web安全构建方案之安全配置apache服务器
 - 5.4 web安全构建方案之web服务访问控制
 - 5.4.1 访问控制常用配置指令
 - 5.4.2 使用.htaccess文件进行访问控制
 - 5.5 web安全构建方案之使用认证和授权保护apache
 - 5.5.1 认证和授权指令
 - 5.5.2 管理认证口令文件和认证组文件
 - 5.5.3 认证和授权使用实例
 - 5.6 web安全构建方案之使用apache中的安全模块
 - 5.6.1 apache服务器中与安全相关的模块
 - 5.6.2 开启安全模块
 - 5.7 web安全构建方案之使用ssl保证web通信安全
 - 5.7.1 ssl简介
 - 5.7.2 apache中运用ssl的基本原理
 - 5.7.3 使用开源的openssl保护apache通信安全
 - 5.8 web安全构建方案之apache日志管理和统计分析
 - 5.8.1 日志管理概述
 - 5.8.2 日志相关的配置指令
 - 5.8.3 日志记录等级和分类
 - 5.8.4 使用wealizer对apache进行日志统计和分析
 - 5.9 web安全构建方案之其他有效的安全措施
 - 5.9.1 使用专用的用户运行apache服务器
 - 5.9.2 配置隐藏apache服务器的版本号
 - 5.9.3 设置虚拟目录和目录权限
 - 5.9.4 使web服务运行在“监牢”中
 - 5.10 web安全构建方案之将黑客拒之门外
 - 5.10.1 web系统风险分析
 - 5.10.2 方案的原则和思路
 - 5.10.3 网络拓扑及要点剖析
 - 5.11 总结
- 第6章 顺手牵羊：窥探ftp安全问题
 - 6.1 数据部门提出的ftp安全需求
 - 6.2 窥探ftp服务存在的安全问题
 - 6.3 使用vsftpd快速构建安全的ftp服务
 - 6.3.1 vsftpd安装

<<蜕变：从菜鸟到Linux安全专家>>

- 6.3.2 vsftpd快速配置
- 6.3.3 vsftpd用户管理
- 6.3.4 vsftpd的高级使用方法
- 6.4 总结
- 第7章 扬名立万：解决电子邮件安全问题
 - 7.1 新的任务：解决电子邮件系统中的安全问题
 - 7.2 电子邮件系统的组成原理
 - 7.2.1 邮件传递代理（mta）
 - 7.2.2 邮件存储和获取代理（msa）
 - 7.2.3 邮件客户代理（mua）
 - 7.3 电子邮件传输协议原理
 - 7.3.1 smtp的模型
 - 7.3.2 smtp的基本命令
 - 7.4 安全配置sendmail电子邮件服务器
 - 7.5 安全配置使用qmail邮件服务器
 - 7.6 安全postfix电子邮件服务器
 - 7.6.1 安全配置postfix邮件服务器
 - 7.6.2 postfix使用smtp安全认证
 - 7.7 防治垃圾邮件的主流策略和技术
 - 7.8 总结
- 第8章 紧急驰援：部署代理服务
 - 8.1 紧急任务：设置代理服务
 - 8.2 代理服务器原理
 - 8.2.1 代理服务器简介
 - 8.2.2 代理服务器的分类
 - 8.3 squid简介
 - 8.4 安装和启动squid server
 - 8.5 安全配置squid server
 - 8.5.1 配置squid server的基本参数
 - 8.5.2 配置squid server的安全访问控制
 - 8.5.3 配置squid server的简单实例
 - 8.6 安全配置基于squid的透明代理
 - 8.7 安全配置多级缓存改善proxy服务器的性能
 - 8.7.1 多级缓存（cache）简介
 - 8.7.2 配置多级缓存
 - 8.8 squid日志管理
 - 8.8.1 配置文件中有关日志的选项
 - 8.8.2 日志管理主文件——access.conf
 - 8.9 在客户端使用squid server
 - 8.9.1 在ie浏览器中设置
 - 8.9.2 在linux下的mozilla浏览器中设置
 - 8.10 配置带认证的代理服务
 - 8.11 配置反向代理服务器
 - 8.11.1 反向代理服务器原理
 - 8.11.2 使用squid配置反向代理服务器
 - 8.12 总结
- 第9章 黎明前的黑暗：做好远程监控和管理

<<蜕变：从菜鸟到Linux安全专家>>

- 9.1 一劳永逸，搞定远程监控和管理
- 9.2 远程监控和管理概述
 - 9.2.1 远程监控与管理的原理
 - 9.2.2 远程监控与管理的主要应用范围
 - 9.2.3 远程监控及管理的基本内容
 - 9.2.4 远程监控及管理的软、硬件要求
- 9.3 使用ssh安全远程访问
 - 9.3.1 ssh服务简介
 - 9.3.2 安装最新版本的openssh
 - 9.3.3 安全配置openssh
 - 9.3.4 ssh的密钥管理
 - 9.3.5 使用scp命令远程复制文件
 - 9.3.6 使用ssh设置“加密通道”
 - 9.3.7 配置ssh的客户端
 - 9.3.8 配置ssh自动登录
- 9.4 使用xmanager 3.0实现linux远程登录管理
 - 9.4.1 配置xmanager服务器端
 - 9.4.2 配置xmanager客户端
- 9.5 使用vnc实现linux的远程管理
 - 9.5.1 vnc简介
 - 9.5.2 启动vnc服务器
 - 9.5.3 使用vnc viewer实现linux远程管理
 - 9.5.4 使用ssh+vnc实现安全的linux远程桌面管理
- 9.6 使用vpn技术保障数据通信的安全
 - 9.6.1 vpn简介
 - 9.6.2 vpn的分类
 - 9.6.3 linux下的vpn
 - 9.6.4 使用ssl vpn：openvpn
 - 9.6.5 使用ipsec vpn
- 9.7 总结
- 第10章 新官上任“第一把火”：解决共享服务安全问题
 - 10.1 samba服务简介
 - 10.2 安装和启动samba
 - 10.3 安全配置samba服务器的用户信息
 - 10.4 安全配置smb.conf文件
 - 10.5 smb.conf中的选项和特定约定
 - 10.6 使用testparm命令测试samba服务器的配置安全
 - 10.7 使用samba日志
 - 10.8 linux和windows文件互访
 - 10.9 nfs服务概述
 - 10.9.1 nfs基本原理
 - 10.9.2 nfs服务中的进程
 - 10.10 安装和启动nfs
 - 10.11 nfs安全配置和使用
 - 10.11.1 配置nfs服务器
 - 10.11.2 配置nfs客户机
 - 10.11.3 安全使用nfs服务

<<蜕变：从菜鸟到Linux安全专家>>

- 10.12 保证nfs安全的使用原则
- 10.13 总结
- 第11章 新官上任“第二把火”：linux网络防火墙安全解决方案
 - 11.1 防火墙技术简介
 - 11.1.1 防火墙简介
 - 11.1.2 防火墙的分类
 - 11.1.3 传统防火墙技术
 - 11.1.4 新一代防火墙的技术特点
 - 11.1.5 防火墙技术的发展趋势
 - 11.1.6 防火墙的配置方式
 - 11.2 netfilter/iptables防火墙框架技术原理
 - 11.2.1 linux中的主要防火墙机制演进
 - 11.2.2 netfilter/iptables架构简介
 - 11.2.3 netfilter/iptables模块化工作架构
 - 11.2.4 安装和启动netfilter/iptables系统
 - 11.2.5 使用iptables编写防火墙规则
 - 11.3 使用iptables编写规则的简单应用
 - 11.4 使用iptables完成nat功能
 - 11.4.1 nat简介
 - 11.4.2 nat的原理
 - 11.4.3 nat的具体使用方法
 - 11.5 防火墙与dmz的配合使用
 - 11.5.1 dmz原理
 - 11.5.2 构建dmz
 - 11.6 防火墙的实际安全部署建议
 - 11.6.1 方案一：错误的防火墙部署方式
 - 11.6.2 方案二：使用dmz
 - 11.6.3 方案三：使用dmz+二路防火墙
 - 11.6.4 方案四：通透式防火墙
 - 11.7 总结
- 第12章 新官上任“第三把火”：入侵检测方案
 - 12.1 入侵检测技术简介
 - 12.1.1 入侵检测技术的原理简介
 - 12.1.2 入侵检测技术的发展
 - 12.1.3 入侵检测的分类
 - 12.1.4 入侵检测系统分类
 - 12.2 安装和配置snort
 - 12.2.1 安装snort
 - 12.2.2 配置snort
 - 12.3 编写snort规则
 - 12.4 总结
- 后记
- 附录a linux常用命令

<<蜕变：从菜鸟到Linux安全专家>>

章节摘录

版权页：插图：

<<蜕变：从菜鸟到Linux安全专家>>

编辑推荐

《蜕变:从菜鸟到Linux安全专家》：没有学历，也可以成为Linux安全专家！
从菜鸟到Linux安全专家，没有不可逾越的鸿沟，学习Linux安全，学以致用是重点。

<<蜕变：从菜鸟到Linux安全专家>>

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>