

**Broadview**

www.broadview.com.cn



从菜鸟到Linux  
安全专家

© 李洋 编著



电子工业出版社

http://www.phei.com.cn

# 蜕变： 从菜鸟到Linux安全专家

---

©李洋 编著

电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

## 内容简介

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。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。  
版权所有，侵权必究。

## 图书在版编目(CIP)数据

蜕变：从菜鸟到Linux安全专家 / 李洋编著. —北京：电子工业出版社，2011.9

ISBN 978-7-121-14434-9

I. ①蜕… II. ①李… III. ①Linux操作系统—安全技术 IV. ①TP316.81

中国版本图书馆CIP数据核字(2011)第172688号

策划编辑：张春雨

责任编辑：李云静

特约编辑：孙佳志

印刷：北京天宇星印刷厂

装订：三河市皇庄路通装订厂

出版发行：电子工业出版社

北京市海淀区万寿路173信箱 邮编：100036

开本：787×1092 1/16 印张：30.75 字数：787.2千字

印次：2011年9月第1次印刷

印数：4000册 定价：75.00元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：(010) 88254888。

质量投诉请发邮件至zltts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

服务热线：(010) 88258888。

# 前言

## 写作目的

“我是一名刚毕业的大学生，想从事Linux安全管理工作，不知道要学些什么？”

“很多企业目前都使用Linux，那么Linux安全怎么管理，要用到哪些技术？”

“我没有很好的学历，学习Linux安全合适吗？能成为合格的Linux安全专家吗？”

.....

很多读者通过Blog、邮件、IM等方式与我沟通，问得最多的就是Linux安全方面的问题。学什么，如何学，如何快速地学，如何学以致用，这些都是他们所关心的问题。并且，Linux系统的门槛确实很高，不像Windows那么容易上手和掌握。由于当前社会、企业以及院校对信息安全的关注度都很高，对Linux安全管理员、安全专家的就业需求也很旺盛，因此，有很多不大了解操作系统原理，没怎么接触过Linux的所谓“菜鸟”同志们也加入到学习的队伍中来。

笔者在信息安全、Linux安全管理领域已经摸爬滚打了十几个年头了，感觉非常有必要写这么一本书来奉献给初涉Linux安全领域的读者们，不但教会他们要用什么技术，而且通过一些小故事来教会他们如何应用这些技术，也就是所谓的安全理念。

总而言之，本书的写作目的是要说明以下几点。

- (1) 没有学历，也可以成为Linux安全专家。
- (2) 从菜鸟到Linux安全专家，没有不可逾越的鸿沟。
- (3) 学习Linux安全，学以致用是重点。

## 本书写作特色

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领域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。Linux作为一种优秀的开源网络操作系统，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，一些大型的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。针对该系统的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及众多操作系统用户的迫切需求。

放眼目前Linux安全技术书籍市场，不难发现，以特定版本Linux为主线进行讲述的书籍比较多，而且比较着重于技术本身。近一年多来，我一直跟电子工业出版社的多位编辑以及广泛的读者进行过很多次交流，一致认为，Linux安全在强调技术的同时，更加强调其应用场景和理念，即不但要解决能用什么技术，更要解决如何用和怎么用的问题，即不但要“授之以鱼”，更要“授之以渔”。原因很简单，在这个知识“爆炸”和Linux操作系统升级版本更新频繁的时代，相对于以前以技术和操作步骤为主流的灌输式论述方法来说，如何掌握知识的本质和有效应用才是当前读者关注的重点。

基于上述考虑，本书独树一帜，以一个刚从学校毕业，走向社会就业的大学生从底层管理员成为公司Linux安全专家成长历程的形式，运用幽默、风趣的故事表现手法，从Linux系统安全和Linux网络安全两个层面系统、全面地向读者介绍作为Linux安全管理员所应具备的方方面面的安全知识、安全原理和安全技能，主要包括Linux文件系统安全、进程安全、Web服务安全、FTP服务安全、防火墙、入侵检测系统等。同时，在故事中也穿插和渗透了关于这些Linux安全技术的应用场景、方法和原则，使读者在故事中全面、系统地掌握Linux安全的技术知识、应用方法和安全理念等。更重要的是，读者还能从故事主人公的职场成长历程中看到和学到Linux安全管理员、Linux安全专家的职业前景和发展轨迹。

本书面向众多的操作系统技术、网络技术工作者，包括系统管理员、网络工程师、网络管理员、网络安全工作者。本书亦可作为高等院校信息安全和操作系统方向的参考教材。

本书的作者有多年从事信息安全、Linux系统研究及开发的工作经验，在精心编写本书的同时还十分考究内容的编排、章节的组织以及讲解的方式，是作者多年理论研究和实践工作经验的结晶。本书由李洋主持编写，其他参与编写的作者还包括王俊丽、谷云、郭瑞、朱振华、魏铮、赵丹、朱耀、卢业伟、丁凡、叶靖、杨文勇、黄江洪、陈亮等，全书由李洋统一组稿和审校。当然，由于作者水平和时间有限，书中难免存在疏漏与不当之处，敬请专家和广大读者给予批评指正。非常欢迎读者访问我的专家博客：<http://patterson.blog.51cto.com/>，与我进行交流互动。

## 本书内容

本书包括12章，并外加引子和1个附录。

引子：以故事为引子，介绍本书的开始情节和背景。

第1章：详细介绍Linux安全的基本理论和背景知识。

第2章：介绍企业级漏洞检测及防范的技术和工具。

第3章：整体、系统地介绍Linux系统防护中进程、文件、用户管理、日志管理的技术

和方法。

第4章：介绍构建安全DNS基础设施的相关技术和方法。

第5章：系统介绍安全构建Web服务器的方方面面。

第6章：详细介绍安全构建FTP服务器的技术和方法。

第7章：介绍安全构建邮件服务的技术和方法，包括垃圾邮件过滤和服务器安全配置等。

第8章：详细介绍代理服务的安全构建方法。

第9章：详细介绍远程监控和管理的技术和方法，包括SSH、VNC、VPN构建等。

第10章：介绍Linux系统下共享资源安全管理的方法，包括Samba、NFS等。

第11章：详细介绍Linux系统下使用IPtables开源防火墙构建网络安全的技术、理念和方法。

第12章：详细介绍Linux系统下使用Snort进行入侵检测的技术和方法。

附录A：推荐和介绍Linux系统下百余个常见的命令，供读者在实际工作中参考。

## 致谢

作者首先由衷地感谢电子工业出版社的编辑张春雨和符隆美，他们在我写书的过程中给了我无私的帮助。为了使本书能尽快与读者见面，他们花费了大量的心血和精力，并对本书质量和体系的把握起到了重要作用。除此之外，还感谢5ICTO网站以及该网站安全频道资深编辑王文文为本书作出的贡献。

李洋

2011年8月于北京

# 目 录

菜鸟前传	1
第1章 上司训话：网络安全态势分析	2
1.1 网络安全概述	3
1.1.1 网络安全问题概览	3
1.1.2 国际大气候	4
1.1.3 信息安全标准化组织及标准	8
1.1.4 我国的实际情况	10
1.2 严峻的网络安全现状	12
1.2.1 黑客入侵	12
1.2.2 病毒发展趋势	12
1.2.3 内部威胁	12
1.2.4 自然灾害	13
1.3 黑客的攻击手段	13
1.4 重大网络安全威胁汇总	16
1.4.1 Scanning	16
1.4.2 木马	17
1.4.3 拒绝服务攻击和分布式拒绝服务攻击	19
1.4.4 病毒	24
1.4.5 IP Spoofing	26
1.4.6 ARP Spoofing	27
1.4.7 Phishing	27
1.4.8 Botnet	30
1.4.9 跨站脚本攻击	31
1.4.10 零日攻击 (Zero Day Attack)	32
1.4.11 “社会工程学”攻击	32
1.5 构建企业安全防范体系 (架构)	34
1.5.1 企业安全防范体系 (架构) 的概念	34
1.5.2 企业安全架构的层次结构及相关安全技术	35
1.5.3 企业安全防范架构设计准则	36

1.6 总结	38
<b>第2章 一举两得：发现企业网络漏洞</b>	<b>39</b>
2.1 正中下怀的任务	40
2.1.1 上司的考验	40
2.1.2 打得啪啪响的如意算盘	40
2.2 发现企业网络漏洞的大致思路	40
2.2.1 基本思路	40
2.2.2 采用网络安全扫描	41
2.3 端口扫描	42
2.3.1 端口扫描技术基本原理	42
2.3.2 端口扫描技术的主要种类	43
2.3.3 快速安装Nmap	46
2.3.4 使用Nmap确定开放端口	47
2.4 漏洞扫描	67
2.4.1 漏洞扫描基本原理	67
2.4.2 选择：网络漏洞扫描或主机漏洞扫描	68
2.4.3 高效使用网络漏洞扫描	69
2.4.4 快速安装Nessus	71
2.4.5 使用Nessus扫描	73
2.5 总结	75
<b>第3章 初露锋芒：制定Linux系统安全保护方案</b>	<b>76</b>
3.1 方案的具体思路	77
3.2 圈定Linux下的重要文件	78
3.3 重要文件的权限设置	80
3.3.1 确定文件/目录访问权限	80
3.3.2 字母文件权限设定法	81
3.3.3 数字文件权限设定法	82
3.3.4 特殊访问模式及粘贴位的设定法	82
3.4 使用文件系统检查工具检查文件系统	84
3.4.1 Tripwire工具简介	84
3.4.2 Tripwire的安装和配置	86
3.4.3 使用Tripwire扫描文件系统改变	93
3.5 保护Linux下的进程安全	97
3.5.1 Linux下的重要进程	98



3.5.2 进程安全管理方法	101
3.5.3 使用进程文件系统管理进程	102
3.6 保证Linux用户管理安全	106
3.6.1 用户密码管理	106
3.6.2 管理用户及组文件安全	111
3.7 做好Linux下的日志管理	117
3.7.1 Linux下的日志分类	117
3.7.2 Linux日志管理的基本命令	118
3.8 总结	122
<b>第4章 SOS:拯救崩溃的企业DNS</b>	<b>123</b>
4.1 事故描述	124
4.2 DNS原理及安全概述	124
4.2.1 DNS简介	124
4.2.2 DNS的组成	125
4.2.3 DNS服务器的类型	126
4.2.4 DNS的工作原理	126
4.2.5 DNS面临的安全威胁	127
4.3 安装和启动DNS服务器	128
4.3.1 安装DNS服务器	128
4.3.2 启动和关闭DNS服务器	129
4.4 安全配置DNS服务器	130
4.4.1 DNS服务器配置文件类型	130
4.4.2 named.conf主配置文件	130
4.4.3 区文件	131
4.4.4 DNS服务器配置实例	133
4.4.5 安全配置DNS客户端	134
4.5 安全使用DNS服务器的高级技巧	136
4.5.1 配置辅助域名服务器	136
4.5.2 配置高速缓存服务器	137
4.5.3 配置DNS负载均衡	138
4.5.4 配置智能DNS高速解析	138
4.5.5 合理配置DNS的查询方式	140
4.5.6 使用dnstop监控DNS流量	142
4.5.7 使用DNSSEC技术保护DNS安全	143

---

4.6 总结 .....	145
<b>第5章 抢班夺权：搞定Web服务器管理权限 .....</b>	<b>146</b>
5.1 Web服务器安全防护大赛 .....	147
5.2 Web安全构建方案之Web服务器选型 .....	147
5.2.1 HTTP基本原理 .....	147
5.2.2 为何选择Apache服务器 .....	148
5.2.3 安装Apache .....	150
5.3 Web安全构建方案之安全配置Apache服务器 .....	151
5.4 Web安全构建方案之Web服务访问控制 .....	156
5.4.1 访问控制常用配置指令 .....	156
5.4.2 使用.htaccess文件进行访问控制 .....	157
5.5 Web安全构建方案之使用认证和授权保护Apache .....	161
5.5.1 认证和授权指令 .....	161
5.5.2 管理认证口令文件和认证组文件 .....	161
5.5.3 认证和授权使用实例 .....	162
5.6 Web安全构建方案之使用Apache中的安全模块 .....	163
5.6.1 Apache服务器中与安全相关的模块 .....	163
5.6.2 开启安全模块 .....	164
5.7 Web安全构建方案之使用SSL保证Web通信安全 .....	165
5.7.1 SSL简介 .....	165
5.7.2 Apache中运用SSL的基本原理 .....	166
5.7.3 使用开源的OpenSSL保护Apache通信安全 .....	170
5.8 Web安全构建方案之Apache日志管理和统计分析 .....	174
5.8.1 日志管理概述 .....	174
5.8.2 日志相关的配置指令 .....	174
5.8.3 日志记录等级和分类 .....	175
5.8.4 使用Webalizer对Apache进行日志统计和分析 .....	177
5.9 Web安全构建方案之其他有效的安全措施 .....	180
5.9.1 使用专用的用户运行Apache服务器 .....	180
5.9.2 配置隐藏Apache服务器的版本号 .....	180
5.9.3 设置虚拟目录和目录权限 .....	183
5.9.4 使Web服务运行在“监牢”中 .....	184
5.10 Web安全构建方案之将黑客拒之门外 .....	186
5.10.1 Web系统风险分析 .....	186

5.10.2 方案的原则和思路	187
5.10.3 网络拓扑及要点剖析	190
5.11 总结	191
<b>第6章 顺手牵羊：窥探FTP安全问题</b>	<b>192</b>
6.1 数据部门提出的FTP安全需求	193
6.2 窥探FTP服务存在的安全问题	193
6.3 使用vsftpd快速构建安全的FTP服务	194
6.3.1 vsftpd安装	194
6.3.2 vsftpd快速配置	194
6.3.3 vsftpd用户管理	199
6.3.4 vsftpd的高级使用方法	200
6.4 总结	205
<b>第7章 扬名立万：解决电子邮件安全问题</b>	<b>206</b>
7.1 新的任务：解决电子邮件系统中的安全问题	207
7.2 电子邮件系统的组成原理	208
7.2.1 邮件传递代理（MTA）	208
7.2.2 邮件存储和获取代理（MSA）	209
7.2.3 邮件客户代理（MUA）	209
7.3 电子邮件传输协议原理	209
7.3.1 SMTP的模型	210
7.3.2 SMTP的基本命令	211
7.4 安全配置sendmail电子邮件服务器	212
7.5 安全配置使用Qmail邮件服务器	221
7.6 安全Postfix电子邮件服务器	222
7.6.1 安全配置Postfix邮件服务器	222
7.6.2 Postfix使用SMTP安全认证	224
7.7 防治垃圾邮件的主流策略和技术	225
7.8 总结	227
<b>第8章 紧急驰援：部署代理服务</b>	<b>228</b>
8.1 紧急任务：设置代理服务	229
8.2 代理服务器原理	229
8.2.1 代理服务器简介	229
8.2.2 代理服务器的分类	231
8.3 Squid简介	232

8.4 安装和启动Squid Server	232
8.5 安全配置Squid Server	234
8.5.1 配置Squid Server的基本参数	234
8.5.2 配置Squid Server的安全访问控制	236
8.5.3 配置Squid Server的简单实例	240
8.6 安全配置基于Squid的透明代理	241
8.7 安全配置多级缓存改善Proxy服务器的性能	243
8.7.1 多级缓存 (cache) 简介	243
8.7.2 配置多级缓存	244
8.8 Squid日志管理	246
8.8.1 配置文件中有关日志的选项	246
8.8.2 日志管理主文件——access.conf	247
8.9 在客户端使用Squid Server	249
8.9.1 在IE浏览器中设置	249
8.9.2 在Linux下的Mozilla浏览器中设置	251
8.10 配置带认证的代理服务	253
8.11 配置反向代理服务器	253
8.11.1 反向代理服务器原理	253
8.11.2 使用Squid配置反向代理服务器	254
8.12 总结	256
<b>第9章 黎明前的黑暗：做好远程监控和管理</b>	<b>257</b>
9.1 一劳永逸，搞定远程监控和管理	258
9.2 远程监控和管理概述	258
9.2.1 远程监控与管理的原理	258
9.2.2 远程监控与管理的主要应用范围	259
9.2.3 远程监控及管理的基本内容	259
9.2.4 远程监控及管理的软、硬件要求	260
9.3 使用SSH安全远程访问	261
9.3.1 SSH服务简介	261
9.3.2 安装最新版本的OpenSSH	263
9.3.3 安全配置OpenSSH	264
9.3.4 SSH的密钥管理	267
9.3.5 使用scp命令远程复制文件	269
9.3.6 使用SSH设置“加密通道”	270

9.3.7 配置SSH的客户端	271
9.3.8 配置SSH自动登录	275
9.4 使用Xmanager 3.0实现Linux远程登录管理	278
9.4.1 配置Xmanager服务器端	278
9.4.2 配置Xmanager客户端	279
9.5 使用VNC实现Linux的远程管理	282
9.5.1 VNC简介	282
9.5.2 启动VNC服务器	282
9.5.3 使用VNC Viewer实现Linux远程管理	284
9.5.4 使用SSH+VNC实现安全的Linux远程桌面管理	285
9.6 使用VPN技术保障数据通信的安全	288
9.6.1 VPN简介	288
9.6.2 VPN的分类	289
9.6.3 Linux下的VPN	292
9.6.4 使用SSL VPN: OpenVPN	295
9.6.5 使用IPSec VPN	299
9.7 总结	306
<b>第10章 新官上任“第一把火”：解决共享服务安全问题</b>	<b>307</b>
10.1 Samba服务简介	308
10.2 安装和启动Samba	309
10.3 安全配置Samba服务器的用户信息	311
10.4 安全配置smb.conf文件	312
10.5 smb.conf中的选项和特定约定	327
10.6 使用testparm命令测试Samba服务器的配置安全	331
10.7 使用Samba日志	332
10.8 Linux和Windows文件互访	332
10.9 NFS服务概述	334
10.9.1 NFS基本原理	335
10.9.2 NFS服务中的进程	337
10.10 安装和启动NFS	337
10.11 NFS安全配置和使用	338
10.11.1 配置NFS服务器	338
10.11.2 配置NFS客户机	339
10.11.3 安全使用NFS服务	341

---

10.12 保证NFS安全的使用原则	342
10.13 总结	343
<b>第11章 新官上任“第二把火”：Linux网络防火墙安全解决方案</b>	<b>344</b>
11.1 防火墙技术简介	345
11.1.1 防火墙简介	345
11.1.2 防火墙的分类	346
11.1.3 传统防火墙技术	348
11.1.4 新一代防火墙的技术特点	349
11.1.5 防火墙技术的发展趋势	351
11.1.6 防火墙的配置方式	352
11.2 Netfilter/Iptables防火墙框架技术原理	353
11.2.1 Linux中的主要防火墙机制演进	353
11.2.2 Netfilter/Iptables架构简介	353
11.2.3 Netfilter/Iptables模块化工作架构	355
11.2.4 安装和启动Netfilter/Iptables系统	356
11.2.5 使用Iptables编写防火墙规则	357
11.3 使用Iptables编写规则的简单应用	359
11.4 使用Iptables完成NAT功能	364
11.4.1 NAT简介	364
11.4.2 NAT的原理	364
11.4.3 NAT的具体使用方法	365
11.5 防火墙与DMZ的配合使用	368
11.5.1 DMZ原理	368
11.5.2 构建DMZ	369
11.6 防火墙的实际安全部署建议	373
11.6.1 方案一：错误的防火墙部署方式	373
11.6.2 方案二：使用DMZ	373
11.6.3 方案三：使用DMZ+二路防火墙	374
11.6.4 方案四：通透式防火墙	375
11.7 总结	375
<b>第12章 新官上任“第三把火”：入侵检测方案</b>	<b>376</b>
12.1 入侵检测技术简介	377
12.1.1 入侵检测技术的原理简介	377
12.1.2 入侵检测技术的发展	377

12.1.3 入侵检测的分类.....	379
12.1.4 入侵检测系统分类.....	380
12.2 安装和配置Snort.....	383
12.2.1 安装Snort.....	383
12.2.2 配置Snort.....	384
12.3 编写Snort规则.....	395
12.4 总结.....	402
后 记.....	403
附录A Linux常用命令.....	404

# 菜鸟前传

小王是一个来自于南方的本科毕业生，年方23，计算机系毕业。怀揣着对首都北京的向往之情，他只身一人来到北京找工作。

先介绍一下小王的背景。小王在上学期比较清闲，于是就自己攒了一台电脑，上上网，聊聊天，编编程，几年下来，虽然文化课成绩不怎么样，但是编程和网络技能长进不小。他很喜欢钻研黑客技术，比如病毒、木马、网络钓鱼等，并且还喜欢上一些网站与BBS，经常在那里学习和讨论。他尤其喜欢研究开源系统下的黑客以及安全技术，为什么呢？因为可以看到源代码。无论是Linux操作系统还是一些开源的黑客工具，他都能修改、使用，这也满足了小王的好奇心。因此，几年下来，小王也算是学校小有名气的“黑客”了。当然，小王并没有搞过什么破坏，据说在上大三的时候，小王发现一家私有企业网站有SQL注入攻击的风险，该企业网站为了奖励他，还给了他500元的奖金。

有了这些基础，小王想找一份能够发挥他专长的工作，这样一来可以提高自己的“黑客”技能，二来可以在开源系统下做一些安全方面的工作。所谓攻防，就是一场永不停止的博弈，小王想从攻与防中不断提升自己。

来到北京后，由于小王毕业的本科院校不是非常著名，因此很多著名的互联网企业都没有挑中他。其实小王的动手能力很强，但是由于上学时没有太注重基础知识的学习，因此一到面试和笔试环节，小王就被刷下来了，他为此感到很烦恼。

功夫不负有心人，经过2个多月的折腾，小王参加了大大小小40多场的招聘会，经过了几十场的面试，他终于被一家小型的网络公司录用为Linux安全运维工程师。

小王就这样开始了他的职业生涯……



# 第1章 上司训话：

## 网络安全态势分析

小王通过重重面试和考核，终于进入了这家网络公司。进公司的第一件事情就是向部门经理报到。部门经理是一个40岁左右的海归，对技术要求比较高，对公司安全管理的要求也很高。这不刚报到完并把手续办好，经理还没跟小王寒暄几句，就交给小王一项艰巨的任务——对网络安全态势作一个分析，小王只有硬着头皮上了，熬了整整3个通宵，终于拿出了一份比较完整的网络安全态势分析报告。

