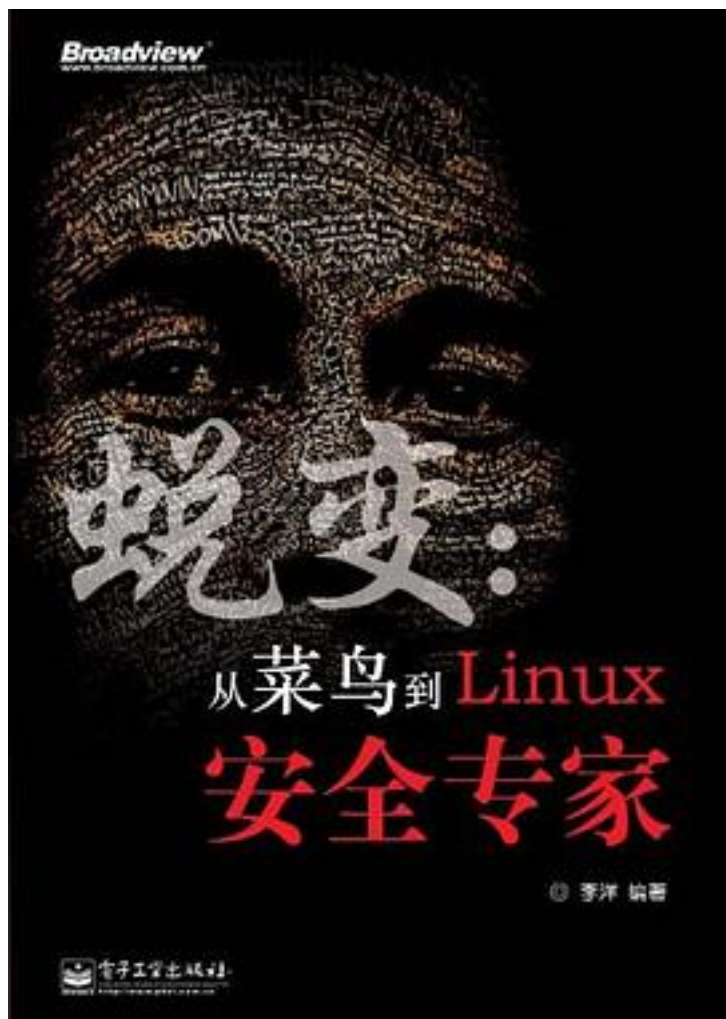


蜕变：从菜鸟到Linux安全专家



[蜕变：从菜鸟到Linux安全专家_下载链接1](#)

著者:李洋 编著

出版者:电子工业出版社

出版时间:2011-9

装帧:平装

isbn:9787121144349

《蜕变:从菜鸟到Linux安全专家》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。《蜕变:从菜鸟到Linux安全专家》覆盖的知识面广，基本覆盖了Linux安全的方方面面。《蜕变:从菜鸟到Linux安全专家》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。《蜕变:从菜鸟到Linux安全专家》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。

作者介绍:

目录: 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 phishing27

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

第2章 一举两得：发现企业网络漏洞39

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nmap46

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
第3章 初露锋芒：制定linux系统安全保护方案	76
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
第4章 sos:拯救崩溃的企业dns	123
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
- 第5章 抢班夺权：搞定web服务器管理权限146
- 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apache150
- 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
- 第6章 顺手牵羊：窥探ftp安全问题192
- 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
- 第7章 扬名立万：解决电子邮件安全问题206
- 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gmail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
- 第8章 紧急驰援：部署代理服务228
 - 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.conf247
 - 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
- 第9章 黎明前的黑暗：做好远程监控和管理257
 - 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openssh263
 - 9.3.3 安全配置openssh264
 - 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: openvpn295
 - 9.6.5 使用ipsec vpn299
- 9.7 总结 306
- 第10章 新官上任"第一把火": 解决共享服务安全问题307
 - 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
- 第11章 新官上任"第二把火": linux网络防火墙安全解决方案344
 - 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
第12章 新官上任"第三把火"：入侵检测方案	376
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
• • • • •	(收起)

[蜕变：从菜鸟到Linux安全专家_下载链接1](#)

标签

Linux

安全

黑客

计算机

IT

计算机文化

电子工业

linux安全

评论

东西比较老，为了引出要讲解的内容时案例也比较生硬。很多安全问题通过后面提出的解决方案实际上也不能很好的解决。所以，这本书只能算可以作为入门书，随便翻阅一下。

安全实例方面的书籍，新手快速上手

linux服务器安全设置

[蜕变：从菜鸟到Linux安全专家 下载链接1](#)

书评

[蜕变：从菜鸟到Linux安全专家 下载链接1](#)