

李洋 编著



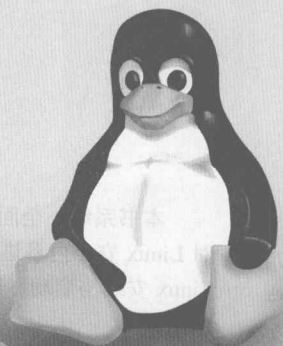
Linux

安全技术内幕

清华大学出版社



李洋 编著



Linux

安全技术内幕

清华大学出版社
北京

内 容 简 介

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。

本书封面贴有清华大学出版社防伪标签，无标签者不得销售。

版权所有，侵权必究。侵权举报电话：010-62782989 13701121933

图书在版编目 (CIP) 数据

Linux 安全技术内幕/李洋编著. —北京：清华大学出版社，2010.7
ISBN 978-7-302-22314-6

I. ①L… II. ①李… III. ①Linux 操作系统—安全技术 IV. ①TP316.89

中国版本图书馆 CIP 数据核字 (2010) 第 055718 号

责任编辑：夏兆彦

责任校对：徐俊伟

责任印制：杨 艳

出版发行：清华大学出版社

地 址：北京清华大学学研大厦 A 座

<http://www.tup.com.cn>

邮 编：100084

社 总 机：010-62770175

邮 购：010-62786544

投稿与读者服务：010-62795954, jsjic@tup.tsinghua.edu.cn

质 量 反 馈：010-62772015, zhiliang@tup.tsinghua.edu.cn

印 刷 者：清华大学印刷厂

装 订 者：三河市李旗庄少明装订厂

经 销：全国新华书店

开 本：190×260 印 张：40 字 数：999 千字

版 次：2010 年 7 月第 1 版 印 次：2010 年 7 月第 1 次印刷

印 数：1~5000

定 价：59.50 元

产品编号：032804-01

FOREWORD

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 Linux 安全的管理和操作中进行对照学习，提高学习效率。

1. 内容安排

第 1 章作为本书的入门知识，详细介绍当前 Linux 网络面临的常见安全威胁，并且本章还将介绍与 Linux 安全相关的网络基础知识。

第 2 章是对 Linux 的概述，着重介绍 Linux 的发展历史、特性、主要应用领域、Linux 内核基本原理等。

第 3 章介绍本书讲解依照的操作系统蓝本——Fedora 10 的安装及启动的相关安全问题，它是学习和掌握本书介绍的 Linux 安全技术的前提。

第 4 章介绍 Linux 用户和组管理的原理以及相关的安全技术。

第 5 章详细介绍保证 Linux 文件系统安全的技术和方法，包括文件/目录访问权限管理和控制、加密文件系统等。

第 6 章从分析 Linux 系统的安全性出发，介绍与之相关的安全原理，并详细介绍使用 Fedora 10 中的 SELinux 机制对 Linux 进行安全增强的技术。

第 7 章对 Linux 的进程安全管理做了详细的介绍，包括进程的基本原理、安全启动与终止、PROC 文件系统以及进程资源限制等。

第 8 章详细介绍了 Linux 日志管理的基本原理、基本命令以及如何使用功能强大的 syslog 设备来安全记录日志。

第 9 章对安全管理 Linux 网络服务的原理和技术进行介绍，包括 xinetd 的使用等。

第 10 章对 DHCP 服务的原理、相关安全配置和使用“牢笼”技术来保证 DHCP 服务安全进行详细介绍。

第 11 章详细介绍如何通过相关配置和技术来安全、高效管理 Linux 下的 DNS 服务。

第 12 章介绍如何在电子邮件服务的搭建过程中有效地避免垃圾邮件等安全威胁，以及如何采用相应的技术和工具来应对这些威胁。

第 13 章对 vsftpd 服务器的安全配置和使用进行详细介绍。

第 14 章针对目前市面上最为流行的 Apache 服务器的安全以及构建安全的 Web 服务器进行详细介绍。

第 15 章详细介绍 Linux 系统中代理服务器——Squid 的安全应用问题，包括访问控制、访问日志管理等。

第 16 章从防火墙的原理、分类以及 Linux 下的 Netfilter/Iptables 防火墙框架的应用几个方面来对防火墙技术进行详细的介绍。

第 17 章着重介绍入侵检测系统的基本原理，并对 Linux 中著名的轻量级入侵检测系统 Snort 进行详细介绍，包括其原理、安装使用以及编写 Snort 规则，并且还对最新的分布式入侵检测系统进行相应介绍。

第 18 章详细介绍集群技术的相关原理和基础，并对 Linux 中非常著名的负载均衡集群——LVS 的安装、配置和使用进行深入的分析 and 介绍。

第 19 章介绍 VPN 技术的基本原理和分类，并深入分析和探讨如何使用开源的 OpenVPN 技术来保障数据通信安全。

第 20 章主要讲述 Linux 下 Samba 服务器的安全使用和配置，从而保证共享资源的安全。

第 21 章对 NFS 服务器的原理进行介绍，并详细介绍 Linux 系统中该服务器的安装、启动、安全配置等问题。

第 22 章详细介绍 PGP 的技术原理，并讨论如何使用开源的 GnuPG 技术来保证数据在网络通信中的安全传输和使用。

第 23 章对 PAM 机制的原理、配置及其应用进行详细介绍，用户可以高效地使用该技术保证 Linux 系统的安全。

第 24 章首先对 Linux 网络安全中经常出现的攻击类型的原理、特点、防范等进行介绍，包括端口扫描、特洛伊木马、拒绝服务攻击 (DoS) 和病毒等，并且还就目前最常见的网络钓鱼、社会工程学攻击的预防给出一些应对策略。最后，还给出了一些常见的有效的备份策略和方法。

第 25 章给用户推荐了多种 Linux 下非常优秀的开源安全工具，使用它们可以更好地辅助用户保护 Linux 系统和网络安全。

附录 A 严格挑选了 100 余种 Fedora 10 中最为常见和重要的命令，并给出了这些命令的功能说明和参数以及语法使用，希望用户作为日常使用和学习的参考。

附录 B 详细介绍本书 Fedora 10 所有操作实例运行的虚拟平台 Vmware 的详细安装和使用过程。

2. 编写分工

本书的编者有多年从事 Linux 安全管理和研发的经验,具有深厚的 Linux 安全基础理论知识和丰富的项目经验。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,争取让读者能够在短时间内掌握 Linux 系统的一些实用的概念和操作,从而能够快速部署和实现 Linux 安全的相关技术和机制。

本书由李洋编著,其他参与部分章节审校和图表处理的还有柴泽楠、靳文佳、张晓明、江扬旺、康宇、宋继阳、吴廷勇、张恒、孙定隆、陈义勇、石依山、姚笃君、李刚、王博、李淞洋、吕远、孙悦、张雷、史思冰、田源、关威等。

由于作者水平有限,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。

编者

2009 年 12 月

CONTENTS

目 录

第 1 章 Linux 安全基础	1
1.1 信息安全的重要性.....	1
1.1.1 网络信息安全的基本概念.....	3
1.1.2 网络威胁的基本表现.....	3
1.1.3 网络信息安全领域的研究重点.....	4
1.1.4 网络信息安全的五要素.....	5
1.1.5 经典的 P2DR 模型.....	6
1.2 黑客攻击的常见手段和步骤.....	6
1.2.1 黑客攻击的常见方法.....	6
1.2.2 黑客攻击的一般步骤.....	7
1.3 Linux 操作系统的安全性.....	10
1.3.1 Linux 操作系统的安全级别.....	10
1.3.2 现行 Linux 操作系统的安全机制.....	12
1.4 Linux 网络安全基础.....	13
1.4.1 网络基本原理.....	13
1.4.2 TCP/IP 网络.....	15
1.4.3 IP 协议.....	17
1.4.4 TCP 协议.....	19
1.4.5 UDP 协议.....	22
1.4.6 ARP 和 RARP 协议.....	23
1.4.7 ICMP 协议.....	24
1.4.8 IPv4 和 IPv6.....	25
1.5 国内外相关安全标准概述.....	27
第 2 章 Linux 概述	30
2.1 Linux 的历史.....	30
2.2 与 Linux 相关的基本概念.....	31
2.2.1 开源软件.....	31
2.2.2 GNU.....	31
2.2.3 GPL.....	32
2.2.4 POSIX.....	33
2.3 Linux 的主要特点.....	33
2.4 Linux 的应用领域.....	34
2.5 Linux 的内核及发行版本.....	35
2.6 常见的 Linux 发行版本.....	35
2.6.1 Red Hat Linux.....	35

2.6.2	Fedora Core/Fedora	36	4.3.2	usermod: 修改用户信息工具	72	
2.6.3	Debian	37	4.3.3	userdel: 删除用户工具	73	
2.6.4	Ubuntu	37	4.3.4	groupadd: 创建组工具	74	
2.6.5	SuSE Linux	38	4.3.5	groupmod: 修改组属性工具	75	
2.6.6	Mandriva	38	4.3.6	groupdel: 删除组工具	76	
2.7	Linux 的主要组成部分	39	4.3.7	其他工具	77	
2.7.1	内核	39	4.4	使用 Fedora 用户管理器管理用户和组	77	
2.7.2	Shell	39	4.4.1	启动 Fedora 用户管理器	77	
2.7.3	文件结构	40	4.4.2	创建用户	78	
2.7.4	实用工具	40	4.4.4	创建用户组	82	
2.8	Fedora Linux 的发展历史	41	4.4.5	修改用户组属性	83	
2.9	Fedora 10 的主要特征	42	4.5	与用户和组管理安全相关的其他安全机制	85	
第 3 章 Fedora 10 的安全安装与启动			44	4.5.1	验证用户和组文件	85
3.1	Fedora 10 的安装	44	4.5.2	用户密码的安全设定方法	87	
3.1.1	硬件需求	44	第 5 章 保证 Linux 文件系统安全			89
3.1.2	安装方式	44	5.1	Linux 文件系统原理	89	
3.1.3	安装过程	45	5.1.1	Linux 中的文件系统类型	89	
3.2	Fedora 10 的启动与登录	56	5.1.2	Linux 文件的类型	92	
3.2.1	安全登录 Linux	57	5.1.3	Linux 中的目录结构设定	93	
3.2.2	退出 Linux	57	5.2	安全设定文件/目录访问权限	95	
3.3	Linux 的启动安全	58	5.2.1	文件/目录访问权限基本概念	95	
3.3.1	Linux 的启动过程	58	5.2.2	改变文件/目录的访问权限	96	
3.3.2	Linux 的运行级别	59	5.2.3	更改文件/目录的所有权	98	
3.3.3	GRUB 密码设定	60	5.2.4	改变文件的执行权限	99	
第 4 章 用户和组安全			62	5.3	使用额外属性保护 Ext3 文件系统安全	100
4.1	用户和组管理的基本概念	62	5.3.1	Ext3 中的额外属性	100	
4.2	安全使用用户和组文件	62	5.3.2	使用 Ext3 文件系统的属性	102	
4.2.1	用户账号文件——passwd	63	5.3.3	Ext3 属性和文件权限的区别	102	
4.2.2	用户影子文件——shadow	64	5.3.4	使用 chattr	104	
4.2.3	组账号文件——group	66	5.4	使用加密文件系统	104	
4.2.4	组账号文件——gshadow	67	5.4.1	内核准备	105	
4.2.5	/etc/skel 目录	68	5.4.2	创建加密设备	106	
4.2.6	/etc/login.defs 配置文件	68	5.4.3	卸载加密设备	109	
4.2.7	/etc/default/useradd 文件	68	5.4.4	重新装载加密设备	109	
4.3	安全管理用户和组工具	70	5.4.5	在 Linux 系统安装时使用 EFS	109	
4.3.1	useradd: 添加用户工具	70				

第 6 章 Linux 系统安全增强技术	111
6.1 Linux 安全增强的经典模型.....	111
6.1.1 BLP 安全模型.....	111
6.1.2 基于角色的访问控制模型.....	112
6.1.3 多级别安全机制.....	113
6.1.4 操作系统安全加固方法.....	114
6.2 SELinux: Linux 安全增强机制.....	115
6.2.1 SELinux 的历史.....	116
6.2.2 SELinux 基本原理.....	116
6.2.3 SELinux 相对于传统机制的 优势.....	117
6.2.4 SELinux 中的上下文.....	117
6.2.5 SELinux 中的目标策略.....	123
6.2.6 使用 SELinux 配置文件和 策略目录.....	134
6.2.7 使用 SELinux 的先决条件.....	136
6.2.8 SELinux 中的布尔变量.....	140
第 7 章 Linux 进程安全	143
7.1 Linux 进程的基本原理.....	143
7.1.1 进程类型.....	143
7.1.2 进程的状态.....	143
7.1.3 进程的工作模式.....	144
7.1.4 进程与线程的区别.....	145
7.2 Linux 下的守护进程.....	145
7.2.1 守护进程基本原理.....	145
7.2.2 Linux 下的重要守护进程.....	146
7.3 安全管理 Linux 进程.....	147
7.3.1 手工启动 Linux 进程.....	147
7.3.2 自动执行进程.....	148
7.3.3 资源空闲时执行进程.....	150
7.3.4 周期性执行进程.....	150
7.3.5 操作 cron 后台进程.....	151
7.3.6 挂起及恢复进程.....	153
7.4 查看及终止进程.....	154
7.4.1 使用 ps 命令查看进程状态.....	154
7.4.2 使用 top 命令查看进程状态.....	156
7.4.3 使用 kill 命令终止进程.....	157
7.4.4 使用 sleep 命令暂停进程.....	158
7.5 安全管理每个进程的系统资源.....	158
7.5.1 限制进程创建大型文件.....	158
7.5.2 限制单个用户调用的最大子 进程个数.....	160
7.6 进程文件系统 PROC.....	161
第 8 章 Linux 日志管理安全	164
8.1 Linux 日志管理简介.....	164
8.2 Linux 下重要日志文件介绍.....	165
8.2.1 /var/log/boot.log.....	165
8.2.2 /var/log/cron.....	166
8.2.3 /var/log/maillog.....	166
8.2.4 /var/log/syslog.....	166
8.2.5 /var/log/wtmp.....	168
8.2.6 /var/run/utmp.....	168
8.2.7 /var/log/xferlog.....	168
8.3 Linux 下基本日志管理机制.....	169
8.3.1 who 命令.....	169
8.3.2 users 命令.....	170
8.3.3 last 命令.....	171
8.3.4 ac 命令.....	172
8.3.5 lastlog 命令.....	173
8.4 使用 syslog 设备.....	173
8.4.1 syslog 简介.....	173
8.4.2 syslog 配置文件.....	173
8.4.3 syslog 进程.....	175
8.5 Linux 日志使用的重要原则.....	176
8.6 Linux 日志输出查看方式.....	176
8.6.1 dmesg.....	176
8.6.2 tail.....	177
8.6.3 more 和 less.....	178
8.6.4 其他方式.....	179
第 9 章 xinetd 安全管理 Linux 网络 服务	180
9.1 xinetd 原理.....	180
9.2 xinetd 服务配置文件.....	181
9.3 通过文件配置使用 xinetd.....	183
9.4 通过图形用户界面进行配置使用 xinetd.....	184

第 10 章 DHCP 服务安全	185
10.1 DHCP 原理.....	185
10.1.1 DHCP 简介.....	185
10.1.2 DHCP 的工作流程.....	185
10.2 安装和启动 DHCP 服务器.....	186
10.2.1 安装 DHCP 服务器.....	186
10.2.2 启动和关闭 DHCP 服务器.....	187
10.3 安全配置 DHCP 服务.....	188
10.3.1 DHCP 服务器配置文件.....	188
10.3.2 DHCP 服务器配置实例.....	190
10.3.3 指定 DHCP 为指定网卡服务.....	191
10.4 安全配置 DHCP 客户端.....	192
10.4.1 图形界面配置 Linux 客户端.....	192
10.4.2 配置文件配置 Linux 客户端.....	192
10.5 使用 chroot 保证 DHCP 运行安全.....	193
10.5.1 下载和安装 Jail 软件.....	194
10.5.2 使用 Jail 创建 chroot 牢笼.....	195
第 11 章 DNS 服务安全	198
11.1 DNS 域名服务原理简介.....	198
11.1.1 DNS 简介.....	198
11.1.2 DNS 系统组成及基本概念.....	199
11.1.3 DNS 服务器的类型.....	200
11.1.4 DNS 的工作原理.....	200
11.2 安装和启动 DNS 服务器.....	201
11.2.1 安装 DNS 服务器.....	201
11.2.2 启动和关闭 DNS 服务器.....	202
11.3 安全配置 DNS 服务器.....	202
11.3.1 DNS 服务器配置文件类型.....	202
11.3.2 named.conf 主配置文件.....	203
11.3.3 区文件.....	204
11.3.4 DNS 服务器配置实例.....	205
11.3.5 安全配置 DNS 客户端.....	207
11.4 安全使用 DNS 服务器的高级技巧.....	208
11.4.1 配置辅助域名服务器做到 冗余备份.....	208
11.4.2 配置高速缓存服务器提高 DNS 服务器性能.....	210
11.4.3 配置 DNS 负载均衡防止 服务器宕机.....	211
11.4.4 配置智能 DNS 高速解析.....	212
11.4.5 合理配置 DNS 的查询方式 提高效率.....	215
11.4.6 使用 dnstop 监控 DNS 流量.....	216
11.4.7 使用 DNSSEC 技术保护 DNS 安全.....	217
第 12 章 邮件服务安全	220
12.1 邮件系统简介.....	220
12.1.1 邮件传递代理 (MTA).....	220
12.1.2 邮件存储和获取代理 (MSA).....	220
12.1.3 邮件客户代理 (MUA).....	221
12.2 SMTP 介绍.....	221
12.2.1 SMTP 的模型.....	221
12.2.2 SMTP 的基本命令.....	222
12.3 安装与启动 Sendmail.....	223
12.4 安全配置 sendmail.cf.....	224
12.5 安全配置 sendmail.mc 文件.....	227
12.6 防治垃圾邮件.....	228
12.6.1 常用技术.....	228
12.6.2 配置 Sendmail 防范垃圾邮件.....	229
12.6.3 使用 SpamAssassin 防治垃圾 邮件.....	230
第 13 章 FTP 服务安全	234
13.1 FTP 简介.....	234
13.1.1 FTP 协议介绍.....	234
13.1.2 FTP 文件类型.....	235
13.1.3 FTP 文件结构.....	236
13.1.4 FTP 传输模式.....	236
13.1.5 FTP 常用命令.....	236
13.1.6 FTP 典型消息.....	237
13.2 安装和启动 vsftpd 服务器.....	238
13.2.1 安装 vsftpd.....	238
13.2.2 启动和关闭 vsftpd.....	238
13.2.3 安全配置 ftpusers 文件.....	241
13.2.4 安全配置 user_list 文件.....	241

13.2.5	安全配置 vsftpd.conf 文件	242
13.2.6	配置其他一些安全选项	245
13.3	安全使用 vsftpd 服务器	246
13.3.1	匿名用户使用 vsftpd 服务器	246
13.3.2	本地用户使用 vsftpd 服务器	247
13.3.3	虚拟用户使用 vsftpd 服务器	249
13.3.4	配置 vsftpd 服务器中 chroot	252
13.3.5	配置 vsftpd 服务器在非标准 端口工作	252
13.3.6	配置虚拟 FTP 服务器	253
13.3.7	使用主机访问控制	255
第 14 章 Web 服务安全 257		
14.1	Web 服务器简介	257
14.1.1	HTTP 基本原理	257
14.1.2	Apache 服务器简介	258
14.2	安装 Apache 的最新版本	260
14.3	配置 Apache 服务器主文件	260
14.4	使用特定的用户运行 Apache 服务器	265
14.5	配置隐藏 Apache 服务器的版本号	266
14.6	实现访问控制	268
14.6.1	访问控制常用配置指令	268
14.6.2	使用 .htaccess 文件进行访问 控制	269
14.7	使用认证和授权保护 Apache	272
14.7.1	认证和授权指令	272
14.7.2	管理认证口令文件和 认证组文件	273
14.7.3	认证和授权使用实例	274
14.8	设置虚拟目录和目录权限	275
14.9	使用 Apache 中的安全模块	277
14.9.1	Apache 服务器中安全 相关模块	277
14.9.2	开启安全模块	278
14.10	使用 SSL 保证安全	278
14.10.1	SSL 简介	278
14.10.2	Apache 中运用 SSL 的 基本原理	279
14.10.3	安装和启动 SSL	284
14.11	Apache 日志管理	287
14.11.1	日志管理概述	287
14.11.2	日志相关的配置指令	287
14.11.3	日志记录等级和分类	288
14.11.4	几个重要的日志文件	289
第 15 章 代理服务安全 293		
15.1	代理服务器简介	293
15.2	Squid 简介	294
15.3	安装和启动 Squid Server	295
15.3.1	安装 Squid Server	295
15.3.2	启动和关闭 Squid Server	295
15.4	在客户端使用 Squid Server	296
15.4.1	在 IE 浏览器设置	296
15.4.2	在 Linux 浏览器中设置	297
15.5	安全配置 Squid Server	299
15.5.1	配置 Squid Server 的基本参数	299
15.5.2	配置 Squid Server 的安全访问 控制	301
15.5.3	配置 Squid Server 的简单实例	306
15.6	安全配置基于 Squid 的透明代理	306
15.6.1	Linux 内核的相关配置	306
15.6.2	Squid 的相关配置选项	308
15.6.3	iptables 的相关配置	308
15.7	安全配置多级缓存改善 Proxy 服务器 的性能	308
15.7.1	多级缓存简介	308
15.7.2	配置多级缓存	309
15.8	Squid 日志管理	311
15.8.1	配置文件中有关日志的选项	311
15.8.2	日志管理主文件——accesss. conf	312
第 16 章 防火墙技术 315		
16.1	防火墙技术原理	315
16.1.1	防火墙简介	315
16.1.2	防火墙的分类	317
16.1.3	传统防火墙技术	318
16.1.4	新一代防火墙	319

16.1.5	防火墙技术的发展趋势	321	17.8.6	activate/dynamic 规则	357
16.1.6	防火墙的配置方式	323	17.8.7	一些重要的指令	357
16.2	Netfilter/iptables 防火墙框架	323	17.8.8	一些重要的规则选项	358
16.2.1	简介	323	17.8.9	使用 Snort 检测攻击	364
16.2.2	安装和启动 Netfilter/iptables 系统	324	17.9	使用 Snortcenter 构建分布式入侵检测系统	366
16.2.3	iptables 基本原理	326	17.9.1	分布式入侵检测系统的构成	366
16.3	iptables 简单应用	327	17.9.2	系统安装及部署	367
16.4	使用 IPtables 完成 NAT 功能	331			
16.4.1	NAT 简介	331	第 18 章 Linux 集群技术		369
16.4.2	NAT 的原理	332	18.1	集群技术	369
16.4.3	NAT 具体使用	333	18.1.1	集群简介	369
16.5	防火墙与 DMZ	336	18.1.2	集群系统的分类	370
16.5.1	DMZ 原理	336	18.1.3	高可用集群	370
16.5.2	构建 DMZ	337	18.1.4	高性能计算集群	371
			18.2	Linux 中的集群	372
			18.2.1	Linux 集群分类	372
第 17 章 入侵检测技术		341	18.2.2	科学集群	372
17.1	入侵检测系统简介	341	18.2.3	负载均衡集群	374
17.2	入侵检测技术的发展	342	18.2.4	高可用性集群	376
17.3	入侵检测的分类	343	18.3	LVS	377
17.3.1	入侵检测技术分类	343	18.3.1	LVS 原理	377
17.3.2	入侵检测系统分类	345	18.3.2	安装 LVS	381
17.4	Snort 简介	347	18.3.3	配置和使用 LVS	382
17.5	安装 Snort	348			
17.6	Snort 的工作模式	349	第 19 章 VPN 技术		385
17.6.1	嗅探器模式	349	19.1	VPN 技术原理	385
17.6.2	数据包记录器	349	19.1.1	VPN 简介	385
17.6.3	网络入侵检测模式	350	19.1.2	VPN 的分类	386
17.7	Snort 的使用方式	350	19.2	Linux 下的 VPN	388
17.7.1	命令简介	350	19.2.1	IPSec VPN	388
17.7.2	查看 ICMP 数据报文	351	19.2.2	PPP Over SSH	389
17.7.3	配置 Snort 的输出方式	353	19.2.3	CIPE: Crypto IP Encapsulation	389
17.7.4	配置 Snort 规则	353	19.2.4	SSL VPN	390
17.8	自己动手编写 Snort 规则	355	19.2.5	PPTP	390
17.8.1	规则动作	355	19.3	使用 OpenVPN	391
17.8.2	协议	356	19.3.1	OpenVPN 简介	391
17.8.3	IP 地址	356	19.3.2	安装 OpenVPN	391
17.8.4	端口号	356	19.3.3	制作证书	392
17.8.5	方向操作符	357			

19.3.4	配置服务端	396	21.1.2	NFS 服务中的进程	431
19.3.5	配置客户端	398	21.2	安装和启动 NFS	432
19.3.6	配置实例	398	21.2.1	安装 NFS	432
			21.2.2	启动 NFS	432
第 20 章	Samba 共享服务安全	400	21.3	NFS 安全配置和使用	433
20.1	Samba 服务简介	400	21.3.1	配置 NFS 服务器	433
20.1.1	Samba 工作原理	400	21.3.2	配置 NFS 客户机	433
20.1.2	Samba 服务器的功能	401	21.3.3	安全使用 NFS 服务	435
20.1.3	SMB 协议	401	21.4	图形界面安全配置 NFS 服务器	436
20.1.4	Samba 服务的工作流程	401	21.5	保证 NFS 安全的使用原则	439
20.2	安装和启动 Samba	402			
20.3	安全配置 Samba 服务器的用户信息	404	第 22 章	PGP 安全加密技术	441
20.3.1	创建服务器待认证用户	404	22.1	PGP 技术原理	441
20.3.2	将用户信息转换为 Samba 用户信息	405	22.1.1	PGP 简介	441
20.3.3	用户转换	405	22.1.2	PGP 原理	442
20.3.4	Samba 服务器和主浏览器	405	22.2	使用 GnuPG	447
20.4	smb.conf 文件配置详解	406	22.2.1	GnuPG 简介	447
20.4.1	设置工作组	407	22.2.2	安装 GnuPG	449
20.4.2	设置共享 Linux 账户主目录	407	22.2.3	GnuPG 的基本命令	449
20.4.3	设置公用共享目录	408	22.2.4	详细使用方法	451
20.4.4	设置一般共享目录	409	22.2.5	GnuPG 使用实例	459
20.4.5	设置共享打印机	410	22.2.6	相关注意事项	465
20.4.6	具体设置实例	412	第 23 章	PAM 安全认证技术	466
20.5	smb.conf 中的选项和特定约定	421	23.1	PAM 认证机制简介	466
20.6	使用 testparm 命令测试 Samba 服务器的配置安全	425	23.2	Linux-PAM 的分层体系结构	467
20.7	使用 Samba 日志	426	23.2.1	分层体系结构概述	467
20.8	Linux 和 Windows 文件互访	426	23.2.2	模块层	468
20.8.1	Windows 客户使用 Linux 系统共享文件	426	23.2.3	应用接口层	468
20.8.2	用 smbclient 工具访问局域网上的 Windows 系统	427	23.3	Linux-PAM 的配置	469
20.8.3	用 smbclient 工具访问局域网上的其他系统	428	23.3.1	Linux-PAM 单一配置文件的语法	469
			23.3.2	口令映射机制	471
			23.3.3	基于目录的配置形式	472
			23.4	Linux 中常用的 PAM 安全模块	473
			23.5	Linux-PAM 使用举例	481
			23.5.1	使用 Linux-PAM 控制用户安全登录	481
第 21 章	网络文件系统安全	429			
21.1	NFS 服务概述	429			
21.1.1	NFS 基本原理	429			

23.5.2	使用 Linux-PAM 控制 Samba 用户的共享登录	482	25.1.6	使用 Tripwire 进行文件监控	527
23.5.3	使用 Linux-PAM 控制 FTP 用户的登录	482	25.1.7	使用 Tripwire 的原则和注意事项	529
第 24 章 Linux 面临的网络威胁及策略			25.2 John the Ripper: 密码分析及检验工具		
24.1	扫描攻击	485	25.2.1	John the Ripper 简介	529
24.2	木马	488	25.2.2	安装 John the Ripper	530
24.3	拒绝服务攻击和分布式拒绝服务攻击	491	25.2.3	基本命令和实用工具	530
24.3.1	DoS 攻击	491	25.2.4	密码分析及检验	532
24.3.2	DDoS 攻击	494	25.3	dmidecode: 硬件状态监控工具	533
24.4	病毒	496	25.3.1	dmidecode 简介	533
24.4.1	Linux 病毒的起源和历程	496	25.3.2	安装 dmidecode 工具	533
24.4.2	病毒的主要类型	497	25.3.3	监控硬件状态	533
24.5	IP Spoofing	498	25.4	NMAP: 端口扫描工具	535
24.6	ARP Spoofing	498	25.4.1	NMAP 简介	535
24.7	Phishing	499	25.4.2	安装 NMAP	536
24.8	Botnet	501	25.4.3	使用 NMAP 进行多种扫描	537
24.9	跨站脚本攻击	502	25.5	Wireshark: 网络流量捕获工具	541
24.10	零日攻击	502	25.5.1	Wireshark 简介	541
24.11	“社会工程学”攻击	503	25.5.2	使用 Wireshark	541
24.12	使用备份应对网络威胁	505	25.6	NTOP: 网络流量分析工具	545
24.12.1	一些简单实用的备份命令	505	25.6.1	NTOP 简介	545
24.12.2	备份机制和备份策略	506	25.6.2	使用 NTOP	546
第 25 章 Linux 下优秀的开源安全工具			25.7 其他工具		
25.1	Tripwire: 系统完整性检查工具	518	25.7.1	安全备份工具	549
25.1.1	文件完整性检查的必要性	518	25.7.2	Nessus: 网络风险评估工具	552
25.1.2	Tripwire 简介	518	25.7.3	Sudo: 系统管理工具	552
25.1.3	Tripwire 的基本工作原理	519	25.7.4	NetCat: 网络安全界的瑞士军刀	553
25.1.4	安装 Tripwire	521	25.7.5	LSOF: 隐蔽文件发现工具	554
25.1.5	配置 Tripwire	522	25.7.6	Traceroute: 路由追踪工具	554
			25.7.7	XProbe: 操作系统识别工具	555
			25.7.8	SATAN: 系统弱点发现工具	555
			附录 A Fedora 10 命令参考		
			附录 B VMWare 虚拟机安装指南		
			556		
			617		

Linux 作为一种优秀的网络操作系统，在实际的系统和网络应用中将会面临层出不穷的黑客攻击、网络威胁。并且，在遇到这些问题的时候，用户需要根据一定的原则和基础知识对问题进行清晰地判定、分析和解决。因此，Linux 安全基础是用户了解 Linux 安全内幕的基本功，也是非常关键的第一步。基于这个原因，本章将向有意学习 Linux 安全内幕的用户详细介绍当前信息安全的背景、概念、研究重点以及网络信息安全的重要性，并以此为基础详细介绍当前 Linux 网络面临的常见安全威胁。本章还将介绍与 Linux 安全相关的网络基础知识。

1.1 信息安全的重要性

以 Internet 为代表的全球性信息化浪潮日益深刻，信息网络技术的应用正日益普及，应用领域从传统的小型业务系统逐渐向大型、关键业务系统扩展，典型的如网站的信息服务系统、数据库服务器系统、党政部门信息系统、金融业务系统、企业商务系统等。伴随着网络的普及，安全日益成为影响网络效率和功能的重要问题，而 Internet 所具有的开放性、国际性和自由性在增加应用自由度的同时，对信息安全提出了更高的要求，这主要表现在如下几个方面。

- **开放性的网络** 它导致网络的技术是全开放的，任何个人、团体都可能通过各种途径获得，因而网络所面临的破坏和攻击可能是多方面的，例如：可以来自物理传输线路的攻击，也可以对网络通信协议和实现实施攻击；可以是对软件实施攻击，也可以对硬件实施攻击。
- **国际性的网络** 意味着网络攻击不仅仅来自本地网络的用户，它可以来自 Internet 上的任何一个国家或地区的任何一台机器，网络安全所面临的是一个国际化的挑战，它没有国家或者是民族等界限。
- **自由性的网络** 意味着网络最初对用户的使用并没有提供任何的技术约束，用户可以自由地访问网络，自由地使用和发布各种类型的信息。用户只对自己的行为负责，而没有任何的法律限制。

开放、自由、国际化的 Internet 的发展给政府机构、企事业单位带来了革命性的改革和开放，使得它们能够利用 Internet 提高办事效率和市场反应能力，以便更具竞争力。通过 Internet，它们可以从异地取回重要数据，同时又要面对网络开放带来的数据安全的新挑战和新危险。如何保护自己网络中关键信息系统的机密信息不受黑客和商业间谍的入侵，已成为网站系统、政府机构、企事业单位信息化健康发展所要考虑的重要事情之一，同时，这也正是网络信息安全的研究日趋激烈和倍受关注的重要原因之一。

从互联网诞生至今，随着信息技术的迅猛发展和 Internet 的快速普及，尤其是电子政务、电子商务、家庭信息化以及军事信息战等诸多新概念和新领域的提出与应用，计算机与互联网正深刻地改变着传统社会的运行模式。信息网络设施对于国家、企业和个人的重要性日益增强，在不断改变人们传统生活、学习与工作方式的同时也带来了新的问题和挑战，即人类社会网络信息化程度日益增加，对网络依赖性日益增强，因此必须保证信息化社会的正常运转，其中信息网络的安全性是最重要的环节之一。

然而，目前越来越多的网络系统面临攻击和入侵的威胁。CERT (Computer Emergency Response Team) 权威数据表明，从 1988 年起，CERT 报告的安全事件每年以指数级增长。根据报告的事件类型统计，网络仿冒事件数量最多，占有接收事件的 35%，且 2007 年上半年的数量便超出 2006 年全年该类事件的总和 (563 件)，共计 645 件。垃圾邮件的数量达 452 件，占 25%。网页恶意代码事件也已超出 2006 年全年的数量总和 (320 件)，达到 360 件。漏洞事件为 186 件，占 10%。病毒、蠕虫或木马事件达 157 件，占 9%。拒绝服务攻击事件为 13 件，占 1%。2007 年半年内所接收的网络安全事件大大超出去年同期水平，而网络仿冒事件、网页恶意代码事件尤为突出，甚至超出 2006 年全年总数。从这些可以明显看到网络安全问题变得日益严重。

在 Internet 发展初期，少数黑客仅仅出于好奇心或炫耀自己高深技术的目的进入未授权系统，而现在大量黑客因利益驱使盗用资源、窃取机密、破坏网络。同时由于网络的普及和黑客工具软件流行，使得攻击网络所需的技术门槛下降，因而破坏性更大。图 1-1 显示了近 20 年间网络攻击复杂性和所需知识的趋势。

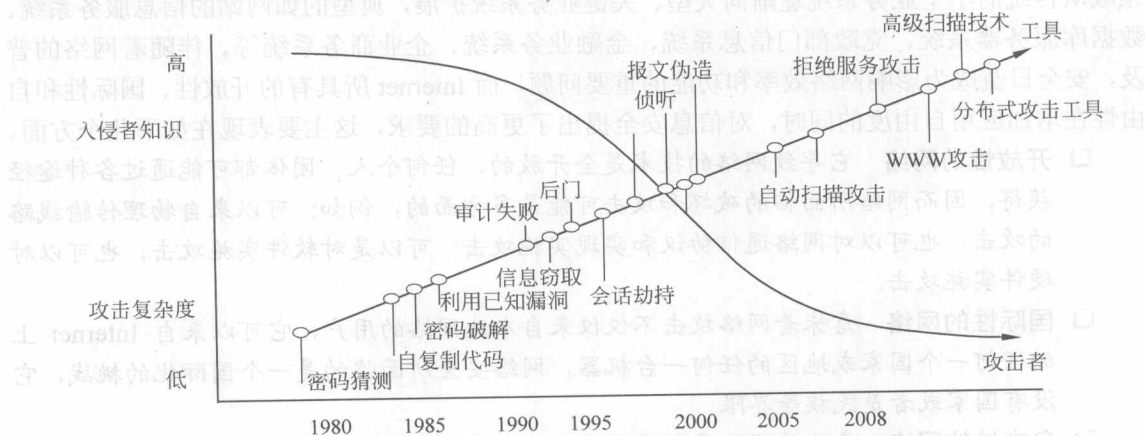


图 1-1 入侵攻击的复杂性与入侵者所需知识程度的关系

从图 1-1 可以看出，在 20 世纪 80 年代，入侵者一般是信息安全领域的专家，拥有深厚的专业知识和独特的入侵攻击手段，很少依靠专用入侵工具。他们一般手工编写入侵代码，对目标系统进行攻击。但是现今由于大量的入侵工具能够从 Internet 上轻松获取，攻击者可以使用这些工具来攻击数以万计的系统。与此同时，攻击类型日益复杂，攻击手段趋向于多样化，入侵和破坏在瞬间完成，同时采取隐藏行踪的手段来逃避检测系统的跟踪，例如，20 世纪 80 年代和 90 年代初期，DoS 事件（拒绝服务攻击）较少报道，并未引起重视，而现在对于电子商务、在线证券交易等网络贸易，DoS 攻击经常造成系统停止运作。另外，在攻击频率高速

增长的同时,攻击者具备的专业知识水平总体在下降,攻击手段却日益复杂,各网络系统都面临严峻考验。据报道,世界平均每 20 秒钟发生一起黑客入侵事件,在美国每年因此造成的经济损失高达 100 多亿美元,涉及政府机构、军事国防、科研院校、金融商业等各部门。计算机网络犯罪已严重干扰了人们的正常生活,造成巨大的经济损失,直接或间接地威胁国家安全。

根据最新的国家计算机网络应急技术处理协调中心的报告,目前网络攻击的动机逐渐从技术炫耀型转向利益驱动型,网络攻击的组织性、趋利性、专业性和定向性继续加强,从而导致为获得经济利益的恶意代码和在线身份窃取成为网络攻击的主流,瞄准特定用户群体的定向化信息窃取和勒索成为网络攻击的新趋势。根据已有资料分析,目前网络攻击从整体上呈现 3 个新的特点。

- **攻击组织严密化** 黑客逐步形成较为严密的组织,致使网络攻击的效率有明显提高。
- **攻击行为趋利化** 针对商业竞争对手的攻击和用于窃取用户账号、密码等敏感数据的网络攻击逐步增多。随着网络行为同社会行为联系的进一步密切,网络攻击的最终目的越来越多地落在获取具体的经济利益上。
- **攻击目标直接化** 网络黑客针对攻击目标的特点,设计特定的攻击代码,绕过网络防御体系入侵有价值的目标主机,或者通过僵尸网络对目标发起直接的大规模网络攻击,使得针对特定目标的网络攻击具有更大的威胁和破坏性。

1.1.1 网络信息安全的基本概念

网络安全是指网络计算机资产的安全,保证其不受自然和人为的有害因素的威胁和迫害。网络安全技术是指各种网络监控和管理技术,这些技术通过对网络系统的硬件、软件以及数据资源进行保护,防止其遭到破坏,保证网络系统能够安全、可靠地运行。它包括 5 个基本要素:机密性、完整性、可用性、可鉴别性与不可抵赖性。

国际标准化组织(ISO)定义计算机信息系统的安全概念为:“为数据处理系统建立和采取的技术和管理的安全保护,保护计算机硬件、软件和数据不因偶然和恶意的原因而遭到破坏、更改和显露。”

1.1.2 网络威胁的基本表现

研究及实践表明,目前网络中存在的对信息系统构成的威胁主要表现在如下几个方面。

- **非授权访问** 没有预先经过同意或认可,就使用网络或计算机资源被看作非授权访问,如有意避开系统访问控制机制,对网络设备及资源进行非正常使用,或擅自扩大权限,越权访问信息等。其主要有以下几种形式:假冒、身份攻击、非法用户进入网络系统进行违法操作、合法用户以未授权方式进行操作等。
- **信息泄露或丢失** 指敏感数据在有意或无意中被泄露出去或丢失。其通常包括信息在传输中丢失或泄露(如黑客们利用电磁泄露或搭线窃听等方式可截获机密信息,或通过对信息流向、流量、通信频度和长度等参数的分析,推出有用信息,如用户口令、账号等重要信息),信息在存储介质中丢失或泄露,通过建立隐蔽隧道等窃取敏感信