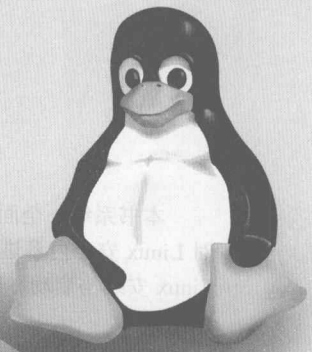
李洋　编著

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。

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，jsjjc@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”，对每个知识点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和介绍。

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，并且还对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，从而能够快速地部署和实现 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

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，占所有接收事件的 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。

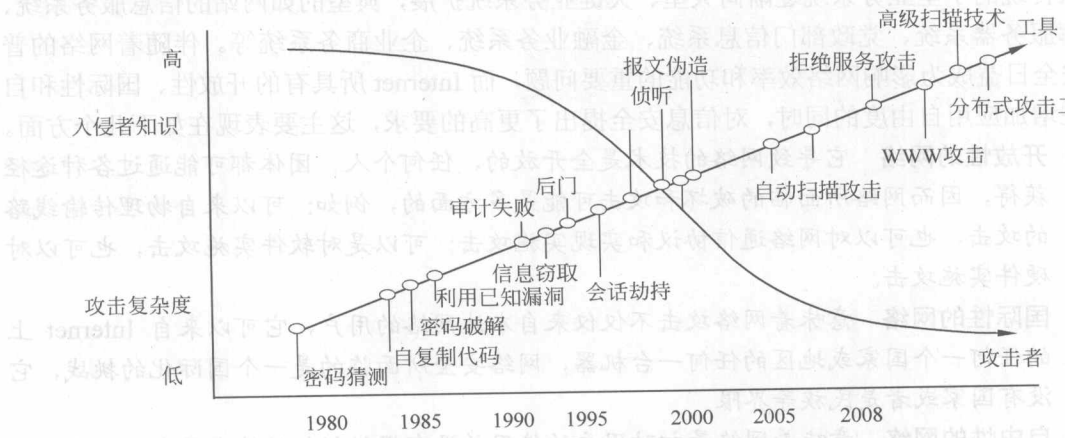


图 1-1　入侵攻击的复杂性与入侵者所需知识程度的关系

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