Hiders

中国计算机学会计算机安全专业委员会推荐参考书

信息与网络安全丛书

Linux 防火墙

[美] Robert L. Ziegler 著

余青霓 周钢 等 译

人民邮电出版社

www.pptph.com.cn

中国计算机学会计算机安全专业委员会推荐参考书

信息与网络安全丛书

Linux 防火墙

[美] Robert L. Ziegler 著

余青霓 周钢 等 译

人民邮电出版社

中国计算机学会计算机安全专业委员会推荐参考书
信息与网络安全丛书

Linux 防火墙

◆ 著　　[美] Robert L.Ziegler
译　　余青霓　周钢　等
责任编辑　李　际

◆ 人民邮电出版社出版发行　北京市崇文区夕照寺街14号
邮编　100061　　电子函件　315@ pptph com cn
网址　http://www.pptph com.cn
北京汉魂图文设计有限公司制作
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销

◆ 开本:787×1092　1/16
印张:24 75
字数:606千字　　2000年10月第1版
印数:1－8 000册　　2000年10月北京第1次印刷

著作权合同登记　图字:01－1999－2055号
ISBN 7-115-08642-7/TP·1717

定价:45.00元

内容提要

作为一名 Linux 用户，虽然你很清楚系统安全的重要性，但却可能没有时间、兴趣或耐性去学习 Linux 安全的每一方面。有了这本书，你无需成为一名安全专家就能快速有效地保护自己的网络不受侵犯，这本书所提供的帮助就和专家一样。

除了介绍设计和实施包过滤防火墙的基本步骤之外，本书还讨论了以下问题：关闭哪些不必要的服务；选择哪些服务作为公共服务；确定哪些本地服务比较危险，需要用防火墙加以保护。本书还提供了有关访问控制的高层形式、通用服务器配置问题、系统安全和完整性监测等方面的信息，用以检测入侵行动发生之前一些初步的刺探活动和进行非授权访问的企图。

本书提供以下信息，可帮助你保护自己的 Linux 网络：

① 一步步地构建一个家庭计算机的单系统包过滤防火墙。

② 构建多系统包过滤防火墙，将 DMZ 网络与专用网分隔开来。

③ 弄清楚哪些服务应该运行、哪些服务不应该运行。

④ 利用 IP 地址隐藏技术，将内部计算机的身份隐藏起来。

⑤ 建立有 tcp wrappers 和 portmap 支持的访问控制列表。

⑥ 有关服务器配置、代理服务器、系统日志和一般系统管理方面的经验。

⑦ 监测系统安全和完整性。

⑧ 当系统安全受到损害后，如何检测并恢复系统。

本书内容新颖、层次分明，特别是对网络安全原理和安全设计作了深入浅出的论述，适合对网络安全感兴趣的各个层次的读者。如果你是一名 Linux 用户，熟悉 Linux 系统，有了这本书，你就会很快成为一名网络安全专家。如果你是一名初学人员，对网络安全有兴趣，你也能从本书中获取许多关于网络安全原理和安全设计的知识。

信息与网络安全丛书 审定委员会

名誉主任：朱恩涛
主　　任：谢模乾
副 主 任：杜肤生
　　顾建国
　　徐修存
委　　员：（以下以姓氏笔划为序）
　　王亚明　冯登国　刘凤昌　吕晓春　杨智慧　屈延文
　　赵世强　赵战生　卿斯汉　高新宇　崔书昆　缪道期

丛书前言

随着科学技术的飞速发展，人们已经生活在信息时代。计算机技术和网络技术深入到社会的各个领域，因特网把“地球村”的居民紧密地连在了一起。如果说“天涯若比邻”在过去只是描写人们心灵上的贴近，那么今天计算机网络已使这句话变成了生活现实。近年来因特网的迅速发展，给人们的日常生活带来了全新的感受，人类社会各种活动对信息网络的依赖程度已经越来越大。

然而，凡事“有一利必有一弊”。人们在得益于信息革命所带来的新的巨大机遇的同时，也不得不面对信息安全问题的严峻考验。1999 年好莱坞推出的以网络为主题的影片《黑客帝国》风靡全球，给人们提示了这个问题的严重性。在人们对网络技术的普及叫好声尚未消失的时候，黑客攻击战在现实生活中也愈演愈烈。国内外众多的网站相继被“黑”，病毒制造者们各显其能。从 CIH 噩梦难醒，到“爱虫”病毒狂吻全球，全球“中毒”者不计其数。这些给各行各业带来了巨大的经济和其他方面损失。除此之外，“电子战”、“信息战”已成为国与国之间、商家与商家之间的一种重要的攻击与防卫手段。因此，信息安全、网络安全的问题已经引起各国、各部门、各行、各业以及每个计算机用户的充分重视。

为了提高我国各级计算机信息网络主管部门的安全意识，普及计算机安全知识，进一步提高国内计算机安全的技术水平，帮助国内技术人员汲取国外计算机安全先进技术和经验，有效保护我国信息网络安全；在公安部公共信息网络安全监察局的大力支持下，我们策划且及时推出了这套《信息与网络安全丛书》。这套丛书采用开放式选题架构，全部是从国外著名出版公司出版的有关信息与网络安全类的权威著作和畅销书中精选而成。这套丛书内容涉及计算机硬件安全、操作系统安全、工作站和服务器的系统安全、网络安全设计、网络入侵检测、网络安全理论等各方面的内容。

由于本套丛书的原版书均是由国外权威人士编写而成，因此在观念上和技术上站在了该领域的前沿。也正因为此，本套丛书受到了有关部门领导和专家的高度重视。由公安部领导和公共信息网络安全监察局及部分计算机安全专家组成的审定委员会对图书进行了审阅，从而保证了丛书的权威性和准确性。当然，由于原版图书所涉及的网络及社会环境等与我国情况不尽相同，读者定会本着批评借鉴的态度结合工作实际进行阅读、参考和分析。

我们真诚希望本套丛书能够为信息与网络安全管理和技术人员提供帮助，为我国的信息安全建设做出贡献。

编者

2000 年 7 月

版权声明

译者序

目前，人类正向一个新的时代——电子信息时代迈进。计算机网络已经渗透到社会生活的各个方面，计算机网络安全问题已经成为影响国家独立和安全，影响经济运行和发展，影响社会稳定和繁荣的重大问题。防火墙则是网络安全中极为重要的一个安全工具。

作为一名 Linux 用户，虽然你很清楚系统安全的重要性，但可能却没有时间、兴趣或是耐性去学习 Linux 安全的每一方面。有了这本书，你无需成为一名安全专家就能快速有效地保护自己的网络不受侵犯，这本书所提供的帮助就和专家一样。

本书的主要翻译工作由余青霓、周钢、马瑞萍等人完成，吴达夫、刘杰、谢剑、张旭铭、马建军、高建堂、常万名、刘向东、韩巍、李朝虎、胡乔等同志也参加了许多讨论和翻译工作。

本书的主要译者近几年来一直从事计算机网络安全方面的研究和开发工作。但正如本书作者所说的："计算机网络安全是一个全新的、快速发展的领域"，再加上国内与国外在信息、技术和工具上的某些差距，整个翻译工作对我们来说是一个不断学习和讨论的过程。译者抱着极其认真和谨慎的态度学习并翻译了全文，在翻译过程中，力求准确，忠实原文，但知识水平和实际经验有限，有误之处敬请读者谅解，并希望给予批评指正。

关于作者

Robert L. Ziegler 毕业于 Wisconsin-Madison 大学心理学专业，随后他又几乎完成德语和哲学的学业。在尝试了几种不同的教育和工作历程之后，他终于决定以自己的爱好为业，又从 Wisconsin-Madison 大学取得了计算机科学的硕士学位。

离开学校后，他加入了一个开发小组，这个队伍是为一家开发小型机的公司工作的，他们曾开发出两种 UNIX 操作系统。Bob 开发出 BSD4.3 UNIX 的多处理器版本，这是开发小组一直努力开发的单处理器版本的一个副产品。从那以后，他就一直在波士顿地区的 R&D 公司从事 UNIX 操作系统的内核开发。

Linux 的出现和用户能够随时访问 Internet 的连接，使 Bob 有机会实现自己从 1982 年起就梦想做的一件事情——在家中拥有自己的 UNIX 服务器和局域网。开始时他只是努力使自己的系统在 Internet 上保持安全，但这种重实用的努力很快就发展成为对 UNIX 家庭用户的热忱，他向公众免费提供基于 Web 的 Linux 防火墙设计服务，还提供了一些流行的防火墙和 LAN 常见问题的解答，帮助人们快速、安全地建立起 Linux 系统。

Bob 现在是诺基亚公司的首席工程师，正在为诺基亚的 Ipsilon 产品系列设计、开发防火墙产品。

关于本书的技术复审人员

Debbie Dailey 目前是一家公司的系统管理员，该公司的管件产品在世界上居于首位。在重返校园以网络安全为重点学习计算机科学之前，她从事了 6 年的大型机工作。Debbie 在参加全日制班的课程时，是系统管理员的实习生，由此开始了她在 UNIX 方面的职业。最近，她从 Purdue 大学取得了计算机科学的理学学士学位。

Craig Hollabaugh 博士自 1985 年第一次进行网上对话以来，就一直喜爱 UNIX。在佐治亚技术研究所攻读交互式模拟仿真专业的电子工程博士学位期间，他管理了几台 Sun 工作站。以后，他在 Texas 大学的流体动力学计算实验室开发了一些接口工具和分布式并行梯度迭代算法的 C++封装程序。1995 年，在他开办的第一家公司——Wireless Scientific，他开发了以 Linux 为中心的工业无线遥测应用软件。后来，由于 Craig 在咨询方面的成功经历，他又到了麻省的 Cambridge，目前他在那儿担任 Kiava Systems 公司的工程副总裁，监管 Kiava 的集成和嵌入式数字信号处理(DSP)硬件的开发工作。他个人的研究兴趣在于数学及科学基础教育中的交互式仿真技术。

致 谢

我一直不理解人们为什么总要在书中写些致谢的话，有谁会去看它们呢？而现在我多少有些明白了。

我要谢谢 Bill Sommerfeld，当他发现我毫无头绪时，给予我所受到的第一次单独辅导；感谢 Gary Zaidenweber 不断向我灌输安全需要，并在开始时帮我建立自己的系统；感谢在惠普公司的其他一些朋友，是他们鼓励我追随自己的理想，尤其是 Mary MacGregor 和我的经理 Cindy Buher，他们也许并不知道我对他们有多么感激；感谢 Paul Fox 在我最初开始时将自己的防火墙拷贝送给我；感谢 Craig Hollabaugh 牺牲数周时间复审书中的问题解答，这本书正是由这些问题产生的；感谢 Karl Runge 牺牲数周时间复审书中的防火墙规则；感谢 NoerthEast Mediaone 新闻组中的众多客户；感谢我的母亲，在我一年多为改变职业方向的问题而奋斗时，她始终相信我能找到属于自己的道路；感谢 Jonathan Kaplan，他一直给我信心和支持；感谢 Old Person，在过去的数年里，他一直是个坚定的朋友，不断地给我鼓励；感谢 Alan Small 的好心，重新整理了此书中最难的那部分内容。最后还要好好谢谢我的编辑 Kitty Jarrett，她说话很温柔，从不横加指责，只是观察并提出问题，而且还常常带些幽默。

前　言

Linux 在家庭业余爱好者和小型的、基于家庭的商业领域中正变得越来越流行和受人欢迎。随着电话线调制解调器和 ASDL 连接服务扩展到消费者市场，直接访问 Internet 在家庭中正变得更加普及。

UNIX 不但是一个流行的服务器平台，特别是作为 Web 服务器的平台，而且它对于家庭局域网(LAN)来说还是一个极好的网关。在这台网关后面，持续不断地连接到 Internet 的是其它的 UNIX 机器、Windows 和 NT 平台、Macintoshes 以及共享的打印机。结果，小型系统用户就被暴露在了他们以前从未需要考虑的安全问题面前。

网络安全对于拥有直接 Internet 连接的 Linux 用户来说是一个特别重要的问题。不像一个简单的个人计算机系统，UNIX 是一个完善的、强有力的操作系统，它的建造目的和主要思想是在一个研究和开发环境中促进信息共享。正因为如此，它才成长成为一个大型而神秘的系统，它不适用于经验缺乏者或不加防备的地方。

将 UNIX 系统连接到 Internet 很像向公众广告开放一幢房子，将你的前门敞开，然后去进行一次长期的休假。在没有防范的情况下，非授权的入侵者就会以各种方式进入，而且这将会很快地发生。

普通家庭或小型系统用户没有时间、兴趣或耐心来学习安全的所有方面，因此本书的目标就是帮助家庭和小型商业 Linux 用户快速地获得他们已有的 Internet 安全措施，而不需要变成一个网络安全专家。必要的防范是不难实现的，但是在一个地方找到所有强调如何去做的信息却不是一件容易的工作。

• 本书包含的内容

对于小型系统用户，安全问题几乎是只关心外部安全、保护他们自己免受来自外界的非授权的网络访问。当然这里也有例外，例如，一些家庭或许会关心特定类型的系统以及由他们的孩子所进行的 Interent 访问。但是，那已经是它的扩展部分了。对于最主要的部分，家庭环境被认为是一个可信的环境。

本书指导家庭和小型商业用户学习设计和实现一个包过滤防火墙的基本步骤。然而防火墙仅仅是迈向安全系统的一步，还需要更高级的安全措施。

计算机安全要求多层设防，没有哪一个层次的安全机制自身就是足够了的。每个后继层依赖于它底层所提供的保护。然而，本书致力于禁止不必要的服务，选择服务使之公共化，并且识别需要在防火墙后面保护的本地危险服务。

本书考察了一个需要防火墙保护类型的小型系统，而且这种保护又能容易和经济地在一个小型系统上实施。考察主题包括包过滤的原理，如何去建立自己的防火墙，如何根据防火墙和通信协议把一些服务设置得更加安全，当访问 Internet 时用 IP 地址隐藏功能来隐藏内部计算机的身份，以及确保防火墙是正在起作用等方面。

本书第三部分讨论了访问控制的更高级形式，虽然这不是本书的基本主题。第三部分的主题包括由 tcp_wrappers 和 portmap 支持的访问控制表、服务器配置、代理和一般的系统管理实践等方面。

本书最后讨论了系统安全和完整性监控、入侵发生前的初步刺探和未授权访问企图的检测、检测攻击信号的工具，以及如果发现了系统被攻陷如何去恢复的问题。

本书中的文字和例子是基于 Red Hat Linux 6.0 的。防火墙的例子是以 ipchains 的命令语法写的。由于目前从 ipfwadm 命令向 ipchains 命令的转化正在进行中，并且 Linux 的这两个版本都在使用，所以将 ipfwadm 语法的例子包括在附录 B 中了。

• 本书未包含的内容

大型商业机构需要强调的安全策略和防范规则几乎与小型系统用户所强调的完全相反。外部 Internet 安全只是大型商业机构所面临安全问题的一小部分，据估计大约 90% 的商业级安全攻击是源于内部企业局域网（LAN），而不是来自外部的 Internet。

本书并不试图去讨论内部系统安全，本书没有涉及多用户的大规模局域网（LAN）安全、复杂的代理配置、企业级认证方式和技术、虚拟专用网、加密或商业级防火墙以及网络体系结构等问题。

• 黑客企图：问题的范围

很难估计目前入侵企图的数目，或许这是因为不成功的入侵企图大部分是未被察觉的，许多站点对这已经习以为常了。在 CERT 文档中的估计是入侵企图的增长与 1998 年 Internet 的指数增长一致。

不管实际的数据到底是多少，全球 Internet 黑客企图以及他们的熟练精密程度都是不可否认地增长了的。端口扫描的模式已经从简单的寻找少数常见的安全缺陷的刺探转变成了

对整个服务端口范围的广域扫描。最新式的黑客工具通过 Web 站点、邮件列表和新闻组在 Internet 上共享。黑客狂们使用 Internet Relay Chat 来协调合作组进行扫描和攻击，这样做大大减少了被检测到的危险。新发现的脆弱性被快速地通过 Internet 公开并立即被利用。软件开发商和安全监控组织处于一种永久的与黑客社团的较量中，每一方都努力使自己保持领先于对方一步。

• 黑客要获取什么

那么谁是这些黑客，他们到底希望得到什么？对此没有唯一的答案。

许多被看作是黑客企图的行动实际上是好奇、一个错误、差的软件和差的系统配置所造成的结果。许多黑客活动与好奇的少年和学生有关，许多都起源于被攻陷的系统，特别是大学站点。系统所有者未意识到他或她的计算机正被一群未邀请的客人作为一个操作基地在使用。于是，对于上面所提到的松散合作的黑客组而言，这是一个好的时机。

至于黑客希望获取什么，一些人想要揭开谜底。某些黑客想要自夸能力，某些黑客只是想进入和破坏，某些黑客则是为了切实的利益。想要发动进一步更深入的攻击，最理想的操作基地就是在被攻陷的站点。由于类似的原因，一个被攻陷的站点给发送大量 E-mail 提供了一个基地或系统资源。一个恶意的目标就是找到一个站点来把它建成一个 WAREZ 库。最后，有一个明显的偷窃目的就是窃取软件和其他智力财富。

• 你会失去什么

当一个系统被攻陷后，一般家庭用户最常见的问题就是遇到不便并被吓住了。因为许多黑客会不适当地去删除硬盘驱动器，因此数据丢失是一个常见的问题。数据丢失还涉及那些没有被备份的文件，因为不管系统是否被损害，系统都需要重头开始，重新安装。

丢失服务是另外一个常见的问题，ISP 通常将关闭帐号直到问题被解决。系统所有者实施关键的安全手续之前，首先必须理解安全缺陷并且学会怎样使系统安全化，这是要花费时间的。对于小型商业用户，所有这些结果意味着除了不便之外还有收入损失。

不仅 ISP 将会以怀疑的眼光看待系统所有者，系统所有者还会在那些受到黑客攻击的客户中丧失名誉。如果 ISP 不信任你，那将极有可能把你作为一个顾客给抛弃掉。如果你的站点被认作了是一个 WAREZ 站点，或者如果黑客攻击了某些站点，那么你还可能面对法律传票和社会的责难。

最后，个人信息和财产信息也能被窃取或非法散布。

• 理想世界中的防火墙和黑客

从概念上讲，许多或大多数的黑客企图是能够由 ISP 或网关服务提供者在源头来阻止的。在路由器和网关上应用标准的过滤程序集将抵制大多数这种类型的安全攻击企图。但不幸的是，这只是在一个理想世界里才可行。不仅需要说服任何地方的所有服务提供者，使他们认识到在这项努力中他们的角色和责任的重要性，而且还必须使网络路由器有能力大规模地处理包过滤的额外负荷，这还不仅仅是硬件的问题。

然而，这些过滤程序能够很容易地在家庭和小型商业系统中实现，而没有任何可察觉到的性能降低。这些程序不仅能帮助你维护一个更加安全的站点，而且还将有助于保护其他人免受你的错误的影响。

目 录