

<<Linux防火墙>>

图书基本信息

书名：<<Linux防火墙>>

13位ISBN编号：9787115086426

10位ISBN编号：7115086427

出版时间：2000-10

出版单位：人民邮电出版社

作者：Robert L.Ziegler

页数：371

字数：606

译者：余青霓

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<Linux防火墙>>

内容概要

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控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。

<<Linux防火墙>>

书籍目录

第一部分 基本事项第1章 包过滤防火墙的基本概念1.1 TCP/IP参考网络模型1.2 服务端口：通向系统程序的大门1.3 数据包：IP网络消息1.3.1 IP消息类型:ICMP1.3.2 IP消息类型：UDP1.3.3 IP消息类型:TCP1.4 小结第二部分 包过滤和基本安全标准第2章 包过滤概念2.1 包过滤防火墙2.2 选择一个默认的包过滤策略2.3 拒绝（Reject）和禁止（Deny）一个包2.4 输入包的过滤2.4.1 远程源地址过滤2.4.2 本地目的地址过滤2.4.3 远程源端口过滤2.4.4 本地目的端口过滤2.4.5 输入包的TCP连接状态过滤2.4.6 刺探和扫描2.4.7 拒绝服务攻击2.4.8 过滤输入数据包的各种考虑2.5 输出包的过滤2.5.1 本地源地址过滤2.5.2 远程目的地址过滤2.5.3 本地源端口过滤2.5.4 远程目的端口过滤2.5.5 TCP连接状态的输出过滤2.6 内部专用对公共网络服务2.6.1 保护不安全的本地服务2.6.2 选择要运行的服务2.7 小结第3章 构建和安装防火墙3.1 ipchains：Linux防火墙管理程序3.1.1 防火墙脚本中所使用的ipchains选项3.1.2 源和目的地址选项3.2 初始化防火墙3.2.1 防火墙例子中使用的符号常量3.2.2 删除任何已存在的规则3.2.3 定义默认策略3.2.4 启用回环接口3.2.5 源地址欺骗和其他的不合法地址3.3 ICMP控制和状态消息过滤3.3.1 错误状态和控制消息 3.3.2 ping Echo Request（类型8）和Echo Reply（类型0）控制消息3.4 保护分配在非特权端口上的服务3.4.1 分配给非特权端口的常用本地TCP服务3.4.2 分配给非特权端口的常用本地UDP服务3.5 激活基本的Internet服务3.5.1 允许DNS（UDP/TCP端口53）3.6 激活公用TCP服务3.6.1 E-mail（TCP SMTP端口25，POP端口110，IMAP端口143）3.6.2 访问Usenet新闻服务（TCP NNTP端口119）3.6.3 telnet（TCP端口23）3.6.4 SSH（TCP端口22）3.6.5 ftp（TCP端口21，20）3.6.6 Web服务3.6.7 finger（TCP端口79）3.6.8 whois（TCP端口43）3.6.9 gopher（TCP端口70）3.6.10 WAIS（TCP端口210）3.7 激活公用UDP服务3.7.1 traceroute（UDP端口33434）3.7.2 访问ISP的DHCP服务器（UDP端口67，68）3.7.3 访问远程网络时间服务器（UDP 123）3.8 记录被禁止的输入数据包3.9 禁止访问有问题的站点3.10 激活LAN访问3.10.1 激活LAN对防火墙内部网络接口的访问3.10.2 激活LAN访问Internet:IP转发和地址隐藏3.11 安装防火墙3.11.1 安装带有静态IP地址的防火墙3.11.2 安装带有动态IP地址的防火墙3.12 小结第4章 局域网、多重防火墙和网络防御带4.1 LAN安全相关问题4.2 可信家庭网络的配置选项4.2.1 LAN访问堡垒防火墙4.2.2 LAN访问别的局域网：在多个LAN之间转发本地网络流4.2.3 LAN访问Internet:通过地址隐藏再转发4.3 大型内部网络的安全配置选项4.3.1 划分子网，创建多个网络4.3.2 通过主机地址或端口范围限制内部访问4.3.3 LAN到Internet网络流的地址隐藏4.3.4 端口重定向——透明代理4.3.5 转发从Internet到内部服务器的连接请求4.4 屏蔽子网防火墙样板4.4.1 防火墙实例中的符号常量说明4.4.2 清空隔断（choke）防火墙原有的安全规则4.4.3 定义隔断防火墙的默认策略4.4.4 激活隔断防火墙机器的回环接口4.4.5 源地址欺骗和别的恶意地址4.4.6 过滤ICMP控制和状态信息4.4.7 激活DNS（UDP/TCP端口53）4.4.8 过滤用户认证服务（TCP端口113）4.4.9 E-mail（TCP SMTP端口25、POP端口110、IMAP端口143）4.4.10 访问Usenet新闻组服务（TCP NNTP端口119）4.4.11 Telnet（TCP端口23）4.4.12 SSH（TCP端口22）4.4.13 FTP（TCP端口21和20）4.4.14 Web服务4.4.15 finger（TCP端口79）4.4.16 Whois服务（TCP端口43）4.4.17 gopher服务（TCP端口70）4.4.18 WAIS（TCP端口43）4.4.19 RealAudio和QuickTime服务（端口554）4.4.20 IRC（TCP端口6667）4.4.21 CU-SeeMe（UDP端口7648，7649，24032；TCP端口7648，7649）4.4.22 Quake服务（UDP端口26000以及1025 - 1200）4.4.23 网络时间服务（UDP端口123）4.4.24 远程系统日志（UDP端口514）4.4.25 Choke主机作为本地DHCP服务器（UDP端口67和68）4.4.26 使局域网中主机访问Choke防火墙主机4.4.27 激活IP地址隐藏功能4.4.28 日志记录4.5 小结第5章 调试防火墙规则5.1 常用的防火墙开发技巧5.2 列出防火墙规则5.2.1 ipchains - Linput5.2.2 ipchains - Linput - n5.2.3 ipchains - Linput - v5.2.4 ipchains - Linput - nv5.3 检查输入、输出和转发规则5.3.1 检查输入规则5.3.2 检查输出规则5.3.3 检查转发规则5.4 用单个数据包对防火墙规则进行测试5.5 检查打开的端口5.5.1 netstat - a [-n-p-Ainet] 5.5.2 strobe5.5.3 nmap5.6 调试SSH——一个真实的例子5.7 小结第三部分 系统级安全和监控第6章 检查系统是否正常运行6.1 用ifconfig检查网络接口6.2 用ping命令检查网络连接6.3 用netstat命令检查网络6.4 用ps - ax检查所有进程6.5 系统日志详解6.5.1 日志记录什么以及在何处记录6.5.2 Syslog的配置6.5.3 防火墙日志消息6.5.4 常被刺探的端口6.5.5 常见的端口扫描日志例子6.5.6 自动日志分析软件包6.6 小结第7章 UNIX系统管理相关问题7.1 认证：检查身份7.1.1 Shadow口令7.1.2 MD5口令hash（哈希）法7.1.3 伯克利（Berkeley）rhost认证：hosts.equiv和.rhost文件7.1.4 共享访问中央认证：网络信息服务

<<Linux防火墙>>

(NIS) 7.2 授权：根据身份限定访问权限7.2.1 root帐号访问特权7.2.2 限制访问su7.2.3 tcp_wrappers程序7.2.4 文件和目录权限7.3 特定服务器配置7.3.1 Telnet配置的相关问题7.3.2 SSH配置的相关问题7.3.3 SMTP配置的相关问题7.3.4 DNS配置的相关问题7.3.5 FTP配置相关问题7.3.6 POP服务器相关配置问题7.3.7 DHCP服务器相关配置问题7.3.8 NTP配置的相关问题7.3.9 HTTP CGI脚本配置相关问题7.4 SOCKS：应用层代理防火墙7.5 /etc/passwd和/etc/group文件中的系统帐号7.6 设置PATH变量7.7 /etc/issue.net文件7.8 远程日志7.9 保持软件不断升级7.9.1 从Red Hat处取得系统的错误更改7.9.2 利用mountd进行攻击的例子7.10 小结第8章 入侵检测和事件报告8.1 系统完整性检查工具8.1.1 COPS8.1.2 Crack8.1.3 ifstatus8.1.4 MD58.1.5 SATAN8.1.6 tiger8.1.7 tripwire8.2 系统可能受损的迹象8.2.1 与系统日志有关的迹象8.2.2 与系统配置有关的迹象8.2.3 与文件系统有关的迹象8.2.4 与用户帐号有关的迹象8.2.5 与安全审计工具有关的迹象8.2.6 与系统性能有关的迹象8.3 系统受到安全侵害后应该采取的措施8.4 事件报告8.4.1 为什么要报告事件8.4.2 报告哪类事件8.4.3 向谁报告事件8.4.4 你应提供哪些信息8.4.5 去何处查找更多的信息8.5 小结第四部分 附录附录A 安全资源附录B 防火墙应用实例和支持脚本附录C 词汇表

<<Linux防火墙>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>