

<<Internet防火墙与网络安全>>

图书基本信息

书名：<<Internet防火墙与网络安全>>

13位ISBN编号：9787111062738

10位ISBN编号：7111062736

出版时间：1998-05

出版时间：机械工业出版社

作者：海尔(美)

译者：刘成勇/等

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>

<<Internet防火墙与网络安全>>

书籍目录

- 目录
- 译者序
- 前言
- 第1章 理解TCP/IP
 - 1.1 TCP/IP的历史
 - 1.2 探索地址、子网和主机名
 - 1.2.1 地址类
 - 1.2.2 子网
 - 1.2.3 无类的地址和CIDR
 - 1.2.4 主机名
 - 1.3 操作网络接口
 - 1.4 网络配置文件
 - 1.4.1 /etc/hosts文件
 - 1.4.2 /etc/ethers文件
 - 1.4.3 /etc/networks文件
 - 1.4.4 etc/protocols文件
 - 1.4.5 etc/services文件
 - 1.4.6 /etc/inetd.conf文件
 - 1.5 理解网络访问文件
 - 1.5.1 /etc/hosts.equiv文件
 - 1.5.2 rhosts文件
 - 1.5.3 用户和主机等价
 - 1.6 检查TCP/IP守护程序
 - 1.6.1 slink守护程序
 - 1.6.2 lsocket守护程序
 - 1.6.3 cpd守护程序
 - 1.6.4 行式打印机守护程序 (lpd)
 - 1.6.5 SNMP守护程序 (snmpd)
 - 1.6.6 RARP守护程序 (rarpd)
 - 1.6.7 BOOTP守护程序 (bootpd)
 - 1.6.8 route守护程序 (routed)
 - 1.6.9 域名服务器 (named)
 - 1.6.10 系统记录器 (syslogd)
 - 1.6.11 inetd 超级服务器
 - 1.6.12 RWHO守护程序 (rwhod)
 - 1.7 探索TCP/IP实用程序
 - 1.7.1 管理命令
 - 1.7.2 用户命令
 - 1.8 本章小结
- 第2章 安全
 - 2.1 安全级别
 - 2.1.1 D1级
 - 2.1.2 C1级
 - 2.1.3 C2级
 - 2.1.4 B1级

<<Internet防火墙与网络安全>>

- 2.1.5B2级
 - 2.1.6B3级
 - 2.1.7A级
 - 2.2加拿大安全
 - 2.2.1EAL - 1
 - 2.2.2EAL - 2
 - 2.2.3EAL - 3
 - 2.2.4 EAL - 4
 - 2.2.5EAL - 5
 - 2.2.6EAL - 6
 - 2.2.7EAL - 7
 - 2.3局部安全问题
 - 2.3.1安全策略
 - 2.3.2口令文件
 - 2.3.3影像口令文件
 - 2.3.4拨号口令文件
 - 2.3.5组文件
 - 2.4口令生命期和控制
 - 2.5破坏者和口令
 - 2.6C2安全性和可信任计算基础
 - 2.7理解网络等价
 - 2.7.1主机等价
 - 2.7.2用户等价
 - 2.8定义用户和组
 - 2.9理解许可权限
 - 2.9.1检查标准的许可权限
 - 2.9.2root和NFS
 - 2.10探索数据加密方法
 - 2.10.1如何对口令加密
 - 2.10.2对文件加密
 - 2.11检查Kerberos身份验证
 - 2.11.1理解Kerberos
 - 2.11.2Kerberos的缺点
 - 2.12理解IP电子欺骗
 - 2.13本章小结
 - 2.14致谢
 - 2.15一个例子程序
- ### 第3章 设计网络策略
- 3.1网络安全计划
 - 3.2站点安全策略
 - 3.3安全策略方案
 - 3.4保护安全策略的责任
 - 3.5风险分析
 - 3.6识别资源
 - 3.7识别威胁
 - 3.7.1定义未授权访问
 - 3.7.2信息泄露的危险

<<Internet防火墙与网络安全>>

- 3.7.3无法使用服务
- 3.8网络使用和责任
- 3.9识别谁可以使用网络资源
 - 3.9.1识别资源的正确使用方法
 - 3.9.2确定谁有权授权访问和同意使用
 - 3.9.3确定用户责任
 - 3.9.4确定系统管理员的责任
 - 3.9.5如何处理敏感信息
- 3.10 安全策略遭到违反时的行动计划
 - 3.10.1对违反策略的反应
 - 3.10.2对本地用户违反策略行为的反应
 - 3.10.3反应策略
 - 3.10.4 定义Internet上好公民的责任
 - 3.10.5 与外部组织的联系和责任
- 3.11解释和宣传安全策略
- 3.12识别与防止安全问题
 - 3.12.1访问入口点
 - 3.12.2 不正确配置的系统
 - 3.12.3软件故障
 - 3.12.4内部的人的威胁
- 3.13.5物理安全
- 3.12.6机密
- 3.13实现合算的策略控制
- 3.14选择策略控制
- 3.15使用后退战略
- 3.16检测和监视非授权活动
- 3.17监视系统使用
- 3.18监视机制
- 3.19监视计划
- 3.20报告过程
 - 3.20.1帐户管理过程
 - 3.20.2配置管理过程
 - 3.20.3恢复过程
- 3.21系统管理员问题报告过程
- 3.22 保护网络连接
 - 3.23使用加密保护网络
 - 3.23.1数据加密标准 (DES)
 - 3.23.2crypt
 - 3.23.3保密增强邮件 (PEM)
 - 3.23.4完全保密 (PGP)
 - 3.23.5源身份验证
 - 3.23.6信息完整性
 - 3.23.7使用校验和
 - 3.23.8密码校验和
 - 3.23.9使用身份验证系统
 - 3.23.10使用智能卡

<<Internet防火墙与网络安全>>

- 3.24 使用Kerberos
- 3.25 保持信息更新
- 3.26 邮件列表
 - 3.26.1 Unix安全邮件列表
 - 3.26.2 Risks论坛列表
 - 3.26.3 VIRUS - L列表
 - 3.26.4 Bugtraq列表
 - 3.26.5 ComputerUndergroundDigest
 - 3.26.6 CERT邮件列表
 - 3.26.7 CERT - TOOLS邮件列表
 - 3.26.8 TCP/IP邮件列表
 - 3.26.9 SUN - NETS邮件列表
- 3.27 新闻组
- 3.28 安全响应小组
 - 3.28.1 计算机快速响应小组
 - 3.28.2 DDN安全协调中心
 - 3.28.3 NIST计算机安全资源和反应情报交换所
 - 3.28.4 DOE计算机事故报告能力 (CIAC)
 - 3.28.5 NASA Ames计算机网络安全响应小组
- 3.29 本章小结
- 第4章 一次性口令身份验证系统
 - 4.1 什么是OTP
 - 4.2 OTP的历史
 - 4.3 实现OTP
 - 4.3.1 决定使用OTP的哪个版本
 - 4.3.2 S/KEY和OPIE如何工作
 - 4.4 Bellcore S/KEY版本1.0
 - 4.5 美国海军研究实验室OPIE
 - 4.5.1 获取OPIE源代码
 - 4.5.2 编译OPIE代码
 - 4.5.3 测试编译过的程序
 - 4.6 安装OPIE
 - 4.7 LogDaemon 5.0
 - 4.7.1 获取LogDaemon代码
 - 4.7.2 编译LgDaemon代码
 - 4.7.3 测试编译过的程序
 - 4.7.4 安装LogDaemon
 - 4.7.5 LogDaemon组件
 - 4.8 使用S/KEY和OPIE计算器
 - 4.8.1 Unix
 - 4.8.2 Macintosh
 - 4.8.3 Microsoft Windows
 - 4.8.4 外部计算器
 - 4.9 实际操作OTP

<<Internet防火墙与网络安全>>

- 4.10 有关/bin/login的安全注释
- 4.11 使用OTP和XWindows
- 4.12 获取更多的信息
- 4.13 本章小结
- 第5章 过滤路由器简介
- 5.1详细定义
- 5.1.1危险区
- 5.1.2 OSI参考模型和过滤路由器
- 5.1.3OSI层次模型
- 5.1.4 过滤路由器和防火墙与OSI模型的关系
- 5.2理解包过滤
- 5.2.1包过滤和网络策略
- 5.2.2 一个简单的包过滤模型
- 5.2.3包过滤器操作
- 5.2.4包过滤器设计
- 5.2.5 包过滤器规则和相关
- 5.3本章小结
- 第6章 包过滤器
- 6.1实现包过滤器规则
- 6.1.1定义访问列表
- 6.1.2使用标准访问列表
- 6.1.3使用扩展访问列表
- 6.1.4 过滤发来和发出的终端呼叫
- 6.2检查包过滤器位置和地址欺骗
- 6.2.1放置包过滤器
- 6.2.2 过滤输入和输出端口
- 6.3在包过滤时检查协议特定的问题
- 6.3.1过滤FTP网络流量
- 6.3.2过滤TELNET网络流量
- 6.3.3过滤X - Windows会话
- 6.3.4 包过滤和UDP传输协议
- 6.3.5包过滤ICMP
- 6.3.6包过滤RIP
- 6.4 过滤路由器配置的例子
- 6.4.1学习实例1
- 6.4.2学习实例2
- 6.4.3学习实例3
- 6.5本章小结
- 第7章 PC包过滤
- 7.1基于PC的包过滤器
- 7.1.1 KarlBridge包过滤器
- 7.1.2Drawbridge包过滤器
- 7.2本章小结
- 第8章 防火墙体系结构和理论
- 8.1检查防火墙部件
- 8.1.1双宿主主机

<<Internet防火墙与网络安全>>

- 8.1.2保垒主机
- 8.1.3过滤子网
- 8.1.4应用层网关
- 8.2本章小结
- 第9章 防火墙实现
- 9.1 TCPWrapper
- 9.1.1例子1
- 9.1.2例子2
- 9.1.3例子3
- 9.1.4例子4
- 9.2FireWall - 1网关
- 9.2.1FireWall - 1的资源要求
- 9.2.2FireWall - 1体系结构概览
- 9.2.3FireWall - 1控制模块
- 9.2.4网络对象管理器
- 9.2.5服务管理器
- 9.2.6规则库管理器
- 9.2.7日志浏览器
- 9.2.8FireWall - 1应用程序举例
- 9.2.9FireWall - 1的性能
- 9.2.10FireWall - 1规则语言
- 9.2.11获得FireWall - 1的信息
- 9.3ANSInterLock
- 9.3.1InterLock的资源要求
- 9.3.2InterLock概览
- 9.3.3配置InterLock
- 9.3.4InterLockACRB
- 9.3.5InterLock代理应用程序
- 网关服务
- 9.3.6 ANSInterLock附加信息源
- 9.4 可信任信息系统Gauntlet
- 9.4.1使用Gauntlet配置的例子
- 9.4.2配置Gauntlet
- 9.4.3用户使用Gauntlet防火墙的概况
- 9.5TIS防火墙工具箱
- 9.5.1建立TIS防火墙工具箱
- 9.5.2配置带最小服务的堡垒主机
- 9.5.3安装工具箱组件
- 9.5.4 网络许可权限表
- 9.6本章小结
- 第10章 TIS防火墙工具箱
- 10.1理解TIS
- 10.2在哪里能得到TIS工具箱
- 10.3在SunOS4.1.3和4.1.4下编译
- 10.4在BSDI下编译
- 10.5安装工具箱
- 10.6准备配置

<<Internet防火墙与网络安全>>

- 10.7配置TCP/IP
- 10.8netperm表
- 10.9配置netacl
 - 10.9.1使用netacl连接
 - 10.9.2重启动inetd
- 10.10 配置Telnet代理
 - 10.10.1通过Telnet代理连接
 - 10.10.2主机访问规则
 - 10.10.3验证Telnet代理
- 10.11配置rlogin网关
 - 10.11.1通过rlogin代理的连接
 - 10.11.2主机访问规则
 - 10.11.3验证rlogin代理
- 10.12 配置FTP网关
 - 10.12.1主机访问规则
 - 10.12.2验证FTP代理
 - 10.12.3通过FTP代理连接
 - 10.12.4 允许使用netacl的FTP
- 10.13 配置发送邮件代理smap和smapd
 - 10.13.1安装smap客户机
 - 10.13.2配置smap客户机
 - 10.13.3安装smapd应用程序
 - 10.13.4 配置smapd应用程序
 - 10.13.5为smap配置DNS
- 10.14 配置HTTP代理
 - 10.14.1非代理所知HTTP客户机
 - 10.14.2使用代理所知HTTP客户机
 - 10.14.3主机访问规则
- 10.15配置XWindows代理
- 10.16 理解身份验证服务器
 - 10.16.1身份验证数据库
 - 10.16.2增加用户
 - 10.16.3身份验证外壳authmgr
 - 10.16.4 数据库管理
 - 10.16.5正在工作的身份验证
- 10.17 为其它服务使用plug - gw
 - 10.17.1配置plug - gw
 - 10.17.2plug - gw和NNTP
 - 10.17.3plug - gw和POP
- 10.18 伴随的管理工具
 - 10.18.1portscan
 - 10.18.2netscan
 - 10.18.3报告工具
 - 10.18.4身份验证服务器报告
 - 10.18.5服务拒绝报告
 - 10.18.6FTP使用报告
 - 10.18.7HTTP使用报告

<<Internet防火墙与网络安全>>

- 10.18.8netacl报告
- 10.18.9邮件使用报告
- 10.18.10Telnet和rlogin使用报告
- 10.19 到哪里寻找帮助
- 第11章 BlackHole
- 11.1理解BlackHole
 - 11.1.1系统要求
 - 11.1.2BlackHole核心模块
 - 11.1.3BlackHole扩展模块
- 11.2使用BlackHole进行网络设计
- 11.3使用BlackHole接口
- 11.4理解策略数据库
- 11.5服务、用户和规则
 - 11.5.1规则
 - 11.5.2用户和用户维护
- 11.6配置BlackHole
 - 11.6.1配置内部和外部DNS
 - 11.6.2配置应用程序服务
- 11.7生成报告
- 11.8更多的信息
- 11.9本章小结
- 附录A 工作表列表
- 附录B 信息源
- 附录C 销售商列表
- 附录D OPIE和LogDaem0n手册

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>