

<<网络安全指南>>

图书基本信息

书名：<<网络安全指南>>

13位ISBN编号：9787115088796

10位ISBN编号：7115088799

出版时间：2002-11

出版时间：人民邮电出版社

作者：Peter Norton Mike Stockman

页数：167

字数：272000

译者：潇湘工作室

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>

## <<网络安全指南>>

### 内容概要

本书完整地介绍了有关网络安全的基础知识，其主要内容有：各种不同网络的运作方式，网络潜在的安全漏洞的产生方式；查找和修复网络缺陷；各种网络防火墙的应用方式；不危及网络安全的访问网络方式；拨入访问和虚拟专用网的安全使用；添加身份验证，以阻止口令攻击和网络快客入侵。

通过对本书的学习，读者可以解决常见的网络系统和协议的问题，保证系统工作正常和安全；掌握增强网络安全性的工具的使用方法和技巧，如扫描网络漏洞，对快客设置网络服务的圈套。

无论读者是网络新手还是富有经验的网络高手，都可以从本书中获得所需要的答案、解释和实例。

本书适用于网络管理员和信息安全管理人员。

## 书籍目录

第一部分 识别危险 第1章 网络 and 安全性概述 1.1 什么是安全性 1.1.1 安全性与便利性 1.1.2 为什么网络易受攻击 1.2 关于局域网 1.2.1 局域网简介 1.2.2 有关局域网的安全主题 1.3 关于广域网 1.3.1 广域网简介 1.3.2 有关广域网的安全主题 1.4 关于防火墙 1.4.1 防火墙简介 1.4.2 有关防火墙的安全主题 1.5 关于万维网和HTTP 1.5.1 万维网 1.5.2 Web服务器的安全主题 1.6 关于虚拟专用网 1.6.1 虚拟专用网简介 1.6.2 虚拟专用网连接的安全主题 1.7 关于远程访问和远程控制 1.7.1 远程访问和远程控制 1.7.2 远程访问和远程控制的安全主题 1.8 本章小结 第2章 风险和规划安全性 2.1 安全威胁的主要类型和分类 2.2 拒绝服务攻击 2.2.1 SYN湮没 2.2.2 Land攻击 2.2.3 Smurf攻击 2.2.4 IP地址欺骗 2.2.5 Teardrop (和Bonk/Boink/Nestea/其他) 2.2.6 死亡之ping 2.2.7 其他拒绝服务攻击 2.3 缓冲区溢出 2.3.1 缓冲区的描述 2.3.2 何时缓冲区溢出成为攻击 2.3.3 利用CGI 2.4 特洛伊木马 2.5 入侵者和物理安全性 2.6 拦截传送 2.7 社会工程 2.8 缺乏用户支持 2.9 本章小结 第3章 确定网络风险 3.1 查找网络的安全漏洞 3.1.1 密切注意新闻 3.1.2 使用端口扫描器 3.1.3 使用网络扫描程序 3.1.4 典型的安全漏洞 3.2 使用网络入侵程序 3.3 修补安全性漏洞 3.3.1 教育用户 3.3.2 软件更新和补丁程序 3.3.3 更改软件选项 3.4 隐蔽的安全性 3.5 本章小结 第二部分 安全工具 第4章 关于防火墙 4.1 防火墙的工作方式 4.1.1 包过滤防火墙 4.1.2 有状态(或动态)的包检查防火墙 4.1.3 应用程序代理防火墙 4.1.4 NAT路由器 4.1.5 个人防火墙 4.2 虚拟专用网 4.2.1 优缺点 4.2.2 VPN服务器的来源 4.3 防火墙的设置位置 4.4 DMZ网络 4.5 报告网络攻击尝试 4.6 阻止未授权的传入访问 4.7 阻止未授权的传出访问 4.8 本章小结 第5章 保证用户连接安全 5.1 确定用户需求 5.1.1 没有实际连接到网络上时需要的网络服务 5.1.2 需要使用哪种协议 5.1.3 不在现场时使用哪种连接方式 5.2 拨入网络服务 5.2.1 优缺点 5.2.2 关于远程访问服务器 5.2.3 建立拨入网络访问 5.2.4 认证 5.3 虚拟专用网 5.3.1 优缺点 5.3.2 可用的VPN加密方法 5.3.3 建立VPN服务器 5.4 外部用户的其他Internet服务 5.4.1 外壳和文件访问 5.4.2 安全文件传输选项 5.5 保护电子邮件 5.5.1 VPN和拨入网络连接 5.5.2 邮件服务器拨入 5.5.3 防火墙和邮件服务器的安全访问 5.6 本章小结 第6章 认证和口令 6.1 创建安全的口令 6.1.1 口令长度 6.1.2 口令的复杂性 6.1.3 更改口令的频率 6.1.4 避免重复的口令 6.2 用户守则 6.2.1 守则1: 决不要写下口令 6.2.2 守则2: 使用一个以上的单词构成口令 6.2.3 守则3: 使用短语建立口令 6.2.4 守则4: 决不在别人注视键盘或屏幕时输入口令 6.2.5 守则5: 经常修改口令(即使系统没有要求) 6.2.6 守则6: 如果怀疑口令泄露则立即改变口令 6.2.7 守则7: 不要告诉任何人(包括我)你的口令 6.3 使用内置的认证 6.4 添加额外的或第三方认证 6.4.1 RADIUS和TACACS+ 6.4.2 Kerberos 6.4.3 公开密钥加密方法 6.5 智能卡和一次性口令 6.5.1 智能卡 6.5.2 安全令牌 6.5.3 一次性口令 6.6 本章小结 第三部分 策略与实施 第7章 规划网络 7.1 建立网络前要问的问题 7.1.1 网络上应运行何种服务 7.1.2 需要连接哪些实际站点 7.1.3 将要使用何种操作系统 7.2 建立服务与禁用不必要的服务 7.2.1 需要运行的协议 7.2.2 不安全的服务及其安全替代措施 7.2.3 扫描网络查找安全漏洞 7.3 本章小结 第8章 主要网络操作系统概述 8.1 确保网络服务器安全的步骤 8.2 规划安全性和访问级别 8.2.1 划分安全需要 8.2.2 将用户分成逻辑组 8.2.3 建立维护过程 8.2.4 培训用户 8.3 Windows NT和Windows 2000 8.3.1 主要安全问题 8.3.2 NT安全机制的运行方式 8.3.3 使系统更安全 8.3.4 建立安全访问控制列表策略 8.4 Novell NetWare 5 8.4.1 NetWare安全机制的运行方式 8.4.2 使系统更安全 8.5 UNIX操作系统 8.5.1 主要安全问题 8.5.2 UNIX安全机制的工作方式 8.5.3 使系统更安全 8.6 本章小结 第9章 桌面系统安全性 9.1 用户工作站的问题 9.1.1 共享过多 9.1.2 Web和FTP服务 9.1.3 其他更好的服务 9.2 Windows 95/98/NT工作站 9.2.1 用户连接服务的方式 9.2.2 启用什么和采取的安全预防措施 9.2.3 将Windows桌面系统与网络服务相连 9.2.4 NetBEUI或IP上的Windows网络 9.3 Mac OS 9.3.1 用户如何连接服务 9.3.2 启用什么和采取的安全预防措施 9.3.3 Macintosh桌面系统连接到网络服务 9.3.4 AppleTalk或IP上的AppleShare 9.4 UNIX/Linux 9.4.1 UNIX桌面系统连接到网络服务 9.4.2 其他类UNIX的操作系统服务器 9.5 总体推荐 9.6 本章小结 第10章 网络被侵入的应对措施 10.1 网络入侵检测系统 10.1.1 基于主机的IDS 10.1.2 基于网络的IDS 10.1.3 IDS如何适应网络 10.1.4 IDS的优缺点 10.1.5 IDS的推荐 10.2 关于端口扫描 10.2.1 端口扫描及含义 10.2.2 来自同一网络的重复连接或尝试 10.2.3 何种情况可能已经被端口扫描 10.2.4 已被扫描了端口时应该做什么 10.3 关于活动日志 10.4

活动警告 10.5 如何处理网络入侵 10.5.1 不使用网络通知组织内部 10.5.2 关闭网络漏洞 10.5.3 通知滥用的帐户和系统管理员 10.5.4 备份系统 10.6 诱骗快客(引诱上钩) 10.7 本章小结 附录A 跟踪安全措施的发展 A.1 政府和学术组织 A.1.1 CERT(计算机紧急响应小组) A.1.2 其他计算机事件和安全性教育站点 A.2 制造商的Web站点 A.3 安全性和黑客组织 A.4 新闻组 A.5 附录小结

#### 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>