

图书基本信息

书名：<<Internet/Intranet网络安全结构设计>>

13位ISBN编号：9787302032939

10位ISBN编号：7302032939

出版时间：1999-02

出版时间：清华大学出版社

作者：许锦波

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>

内容概要

内容简介

本书主要讲述Internet/Intranet的安全结构，首先从构成Internet/Intranet的基本部件的安全性着手，分别叙述了它们各自的安全问题和安全措施，然后从总体上介绍一个综合运用各部件的实际安全网络方案，该方案有机地糅合了各个安全部件，从而使大家进一步认清各个安全部件的相互关系。

本书内容覆盖了TCP/IP协议、域名系统、防火墙技术、电子邮件系统、WWW系统、网络管理系统、数据库管理系统和办公自动化系统等各部分的安全。

本书行文流畅、示

例丰富、讲解清晰、介绍全面，必能让读者受益匪浅。

书籍目录

目录

第一章 Internet/Intranet解决方案综述

1.1 概述

1.1.1 Intranet在中国的诞生

1.1.2 Intranet的实质

1.1.3 Intranet解决方案的基本结构

1.1.4 面向业务系统的解决方案

1.2 网络建设背景

1.2.1 系统目标及任务

1.2.2 设计原则

1.3 Internet/Intranet的组成、结构与功能

1.3.1 Intranet的网络逻辑构成

1.3.2 操作系统及应用系统结构逻辑图

1.4 网络系统连接结构

1.4.1 主干网技术的选择

1.4.2 网络拓扑结构

1.4.3 网络通信协议

1.5 本章小结

第二章 TCP/IP介绍

2.1 OSI参考模型

2.2 TCP/IP

2.3 IP层

2.3.1 IP数据包格式

2.3.2 IP地址

2.3.3 子网

2.3.4 网络掩码

2.3.5 IP冲突

2.3.6 IP欺骗攻击的防范

2.3.7 IP层其他控制协议

2.4 TCP和UDP

2.5 应用层

2.6 端口

2.7 本章小结

第三章 标准和非标准的TCP/TP服务

3.1 远程登录

3.2 文件传输协议

3.2.1 FTP

3.2.2 提供匿名FTP服务

3.2.3 TFTP

3.2.4 UUCP

3.2.5 FSP

3.2.6 RCP

3.3 电子邮件

3.4 Usenet新闻

3.5 万维网

- 3.5.1 WWW
- 3.5.2 Gopher
- 3.5.3 广域网信息服务
- 3.5.4 Archie
- 3.6 网上成员信息查询
- 3.6.1 finger
- 3.6.2 whois
- 3.7 实时会议服务
- 3.7.1 talk
- 3.7.2 IRC
- 3.7.3 MBONE
- 3.8 名字服务
- 3.9 网络管理服务
- 3.10 时间服务
- 3.11 NIS系统
- 3.11.1 NIS结构
- 3.11.2 NIS安全脆弱性
- 3.11.3 攻击NIS的例子
- 3.11.4 可能的解决方法.
- 3.12 网络文件系统
- 3.12.1 NFS的协议层次
- 3.12.2 RPC
- 3.12.3 XOR
- 3.12.4 NFS的两个协议
- 3.12.5 客户端的NFS相关进程
- 3.12.6 服务器端的NFS进程
- 3.12.7 从服务器端调出文件系统
- 3.12.8 客户端的相关信息
- 3.12.9 NFS的RPC认证
- 3.12.10 不安全的NFS对系统的危害
- 3.12.11 安全NFS
- 3.13 窗口系统
- 3.14 打印系统
- 3.15 编写安全的守护程序
- 3.15.1 程序安全的重要性
- 3.15.2 SUID/SGID程序的设计
- 3.15.3 root程序的设计
- 3.15.4 编写安全的网络程序
- 3.16 本章小结
- 第四章 广域网络连接技术
- 4.1 广域网的连接力式
- 4.2 连接广域网常用网络设备
- 4.2.1 调制解调器
- 4.2.2 通信服务器
- 4.2.3 网桥和路由器
- 4.3 VSAT
- 4.4 PPP和SLIP

4.4.1 PPP

4.4.2 SLIP

4.5 帧中继

4.6 X.25

4.7 ATM

4.8 路由

4.8.1 静态路由

4.8.2 动态路由

4.8.3 外部路由

4.9 本章小结

第五章 WindowsNT的安全机制

5.1 WindowsNT的安全概述

5.2 WindowsNT中的术语

5.2.1 WindowsNT中的对象

5.2.2 WindowsNT服务器和WindowsNT工作站

5.2.3 工作组

5.2.4 域

5.2.5 域控制器

5.2.6 WindowsNT注册表

5.3 WindowsNT的安全模型

5.3.1 WindowsNT的安全子系统

5.3.2 WindowsNT中的登录上网

5.3.3 登录标志

5.3.4 WindowsNT登录的过程

5.3.5 可根据需要选择的存取控制

5.3.6 存取标识

5.4 WindowsNT环境中的用户帐户

5.5 NT文件系统的安全性

5.6 WindowsNT域

5.7 域委托关系的安全概念

5.8 本章小结

第六章 UNIX系统的安全性

6.1 UNIX的用户帐户

6.2 UNIX文件系统

6.3 UNIX的NIS

6.3.1 NIS与分布环境的管理

6.3.2 NIS组成

6.3.3 NIS映射的数据

6.4 本章小结

第七章 认证和加密

7.1 认证

7.1.1 认证的种类

7.1.2 认证服务器存在的问题

7.1.3 认证服务器的商用解决方案

7.2 网络级加密

7.2.1 加密层次

7.2.2 加密对象

7.2.3 加密地点

7.2.4 密钥分配

7.3 本章小结

第八章 域名系统

8.1 域名系统的结构

8.2 名字服务器

8.3 解析器

8.4 地址到名字的映射

8.5 UNIX名字服务 BIND

8.5.1 named的配置

8.5.2 标准资源记录

8.5.3 缓存初始化文件

8.5.4 自反地址映射文件

8.5.5 反向域文件

8.5.6 名字到地址的转换文件

8.6 名字欺骗技术

8.7 本章小结

第九章 防火墙技术

9.1 Internet上的安全性问题

9.2 防火墙简介

9.3 防火墙的一般组成

9.4 防火墙的不同实现技术

9.4.1 数据包过滤技术

9.4.2 过滤FTP会话

9.4.3 应用层网关

9.4.4 应用层网关的优缺点

9.4.5 代理服务

9.4.6 数据包过滤和代理服务的比较

9.5 网络拓扑结构和防火墙技术的关系

9.6 本章小结

第十章 名字服务器和防火墙的配合

10.1 名字服务器的数据包特性

10.2 名字服务器的代理特性

10.3 分散的名字服务器策略

10.3.1 外部计算机的名字服务器

10.3.2 堡垒主机的名字服务器

10.3.3 内部计算机的名字服务器

10.4 名字服务器的位置

10.5 非透明防火墙网络的名字服务器

10.5.1 内部名字服务的配置

10.5.2 外部名字服务器的配置

10.5.3 堡垒主机的名字服务器配置

10.6 透明防火墙的名字服务器

10.6.1 外部名字服务器

10.6.2 内部名字服务器

10.6.3 数据包过滤

10.7 设置名字服务器来隐藏信息

10.7.1 在堡垒主机上建立伪名字服务器供外界使用

10.7.2 内部名字服务器客户机查询内部服务器

10.7.3 堡垒名字服务器客户机查询内部服务器

10.7.4 数据包过滤

10.8 本章小结

第十一章 穿越防火墙的远程登录和远程执行

11.1 Teinet及它的代理性

11.2 远程命令执行

11.1.2 BSDr命令的数据包特性

11.2.2 BSDr命令的代理特性

11.3 远程执行命令rexec

11.3.1 rexec的数据包过滤特性

11.3.2 rexec的代理特性

11.4 远程执行命令rex

11.4.1 reX的数据包过滤特性

11.4.2 reX的代理特性

11.5 本章小结

第十二章 穿越防火墙的文件传输

12.1 文件传输协议

12.1.1 FTP的数据包特性

12.1.2 FTP的代理特性

12.2 简单文件传输协议

12.2.1 TFTP的数据包过滤特性

12.2.2 TFTP的代理特性

12.3 文件服务协议

12.3.1 FSP的数据过滤特性

12.3.2 FSP的代理特性

12.4 网络文件系统

12.4.1 NFS的数据包过滤特性

12.4.2 NFS的代理特性

12.5 本章小结

第十三章 网络管理服务与防火墙的配合

13.1 简单网络管理协议

13.1.1 SNMP的数据包特性

13.1.2 SNMP的代理特性

13.2 路由信, 协议

13.2.1 RIP的数据包特性

13.2.2 RIP的代理特性

13.3 ping

13.3.1 ping数据包过滤特性

13.3.2 ping的代理特性

13.4 traceroute

13.4.1 traceroute数据包特性

13.4.2 traceroute的代理特性

13.5 其他ICMP数据包

13.6 网络信息服务/黄页

13.6.1 NIS/YP的数据包过滤特性

13.6.2 NIS/YP的代理特性

13.7 网络上的信息查询

13.7.1 finger的数据包过滤特性

13.7.2 finger的代理特性

13.7.3 whois

13.7.4 whois的数据包过滤特性

13.7.5 whois的代理特性

13.8 本章小结

第十四章 穿越防火墙的新闻服务

14.1 NNTP的数据包特性

14.2 NNTP的代理性

14.3 NNTP的数据包过滤

14.4 本章小结

第十五章 防火墙之外

15.1 网络安全检查 SecureTest和securityHeaithCheck

15.2 防火墙安全分析

15.2.1 SecureVIEW体系结构

15.2.2 丰富的分析和报告

15.2.3 灵活的和可定制的输出

15.2.4 SecureVIEW的重要特性

15.3 网络传输内容安全性域网络过滤软件

15.3.1 MIMESweeper

15.3.2 SurfWatch

15.3.3 WebSENSE

15.4 入侵检测和扫描

15.4.1 SAFEsuite

15.4.2 扫描工具

15.4.3 其他

15.5 本章小结

第十六章 电子邮件系统

16.1 电子邮件

16.2 电子邮件的地址

16.3 邮件网关

16.4 邮件格式

16.4.1 非ASC 码数据的MIME扩展

16.4.2 MIME多部分报文

16.5 简单邮件传送协议

16.6 MX记录

16.6.1 MX算法

16.6.2 设置MX记录

16.6.3 构造MX列表

16.7 本章小结

第十七章 企业邮件和Internet的连接

17.1 概述

17.2 邮件网关的选择

17.3 为局域网邮件用户传入邮件

17.4 传出邮件方案

- 17.4.1 传出的局域网邮件方案一
- 17.4.2 传出的局域网邮件方案二
- 17.4.3 传出的局域网邮件方案三
- 17.5 本章小结
- 第十八章 Notes的邮件规划
- 18.1 Notes邮件特性
- 18.2 Domino邮件服务器
- 18.3 Notes邮件的相关概念
 - 18.3.1 网络域
 - 18.3.2 命名网络
 - 18.3.3 公用通讯录
 - 18.3.4 连接文档
 - 18.3.5 邮递表
 - 18.3.6 邮箱
 - 18.3.7 邮件优先级
 - 18.3.8 邮件文件
- 18.4 Notes邮件规划和邮递算法
 - 18.4.1 Notes网络域中邮件传递算法
 - 18.4.2 Domino命名网络中邮件邮递算法
- 18.5 Notes邮件在Internet上的邮递
- 18.6 SMTP/MIMEMTA的结构
 - 18.6.1 SMTP/MIMEMTA任务组件
 - 18.6.2 SMTP/MIMEMTA的数据库
- 18.7 Notes和internet之间的邮件传输
 - 18.7.1 从Notes到Internet的传输
 - 18.7.2 从Internet到Notes传输邮件
- 18.8 配置SMTP/MIMEMTA
 - 18.8.1 MTA 配置的前期准备工作
 - 18.8.2 SMTP/MIMEMTA 和Internet直接连接
 - 18.8.3 通过防火墙或邮件中继系统和Internet连接
 - 18.8.4 通过防火墙和Internet连接同时直接邮递Internet消息
 - 18.8.5 同时使用两个MTA 分别用于Internet消息和Intranet消息
- 18.9 本章小结
- 第十九章 PGP及其安全性
- 19.1 PGP简介
- 19.2 PGP原理
 - 19.2.1 RSA算法
 - 19.2.2 消息文摘
 - 19.2.3 数字签名
 - 19.2.4 PGP的密钥管理
- 19.3 PGP的安全性
 - 19.3.1 IDEA的安全性
 - 19.3.2 RSA的安全性
 - 19.3.3 MD5的安全性
 - 19.3.4 随机数的安全性问题
 - 19.3.5 PGP的密钥和口令的安全性问题
 - 19.3.6 没有完全删除的文件

- 19.3.7 PGP的时间戳可靠性
- 19.3.8 流量分析
- 19.3.9 现实的PGP攻击
- 19.4 本章小结
- 第二十章 WWW的安全性
- 20.1 Web与HTTP协议
 - 20.1.1 Web的访问控制
 - 20.1.2 HTTP安全考虑
 - 20.1.3 安全超文本传输协议
 - 20.1.4 安全套接层
 - 20.1.5 缓存的安全性
- 20.2 WWW服务器的安全漏洞
 - 20.2.1 NCSA服务器的安全漏洞
 - 20.2.2 ApacheWWW服务器的安全问题
 - 20.2.3 Netscape的WWW服务器的安全问题
- 20.3 CGI程序的安全问题
 - 20.3.1 CGI程序的编写应注意的问题
 - 20.3.2 CGI脚本的激活方式
 - 20.3.3 不要依赖于隐藏变量的值
 - 20.3.4 WWW客户应注意的问题
 - 20.3.5 使用Perl的感染检查
 - 20.3.6 Cgi的权限问题
- 20.4 Plug - in的安全性
- 20.5 SSL的加密的安全性
- 20.6 Java与JavaScript
 - 20.6.1 Javaapplet的安全性问题
 - 20.6.2 JavaScript的安全性问题
- 20.7 ActiveX的安全性
- 20.8 Cookies的安全性
- 20.9 本章小结
- 第二十一章 Internet网络管理
- 21.1 网络管理的功能
- 21.2 网络管理概念
- 21.3 网络管理标准
 - 21.3.1 框架标准
 - 21.3.2 功能标准
 - 21.3.3 通信标准
 - 21.3.4 信息标准
- 21.4 网络管理策略
- 21.5 网络管理协议介绍
- 21.6 协议的体系结构
 - 21.6.1 管理信息标准
 - 21.6.2 MIB变量的例子
 - 21.6.3 管理信息结构
- 21.7 AsN.1形式定义
- 21.8 一个标准网络管理协议
- 21.9 SNMP的安全性

- 21.9.1 和安全性相关的概念
- 21.9.2 SNMPV1的安全性问题
- 21.9.3 SNMPV2的安全件
- 21.10 网络管理工具介绍
 - 21.10.1 Netview
 - 21.10.2 Accunaster
 - 21.10.3 Serviceview
- 21.11 本章小结
- 第二十二章 计费解决方案
 - 22.1 拨号接入服务的用户认证、管理和计费系统
 - 22.1.1 用户计费系统的管理
 - 22.1.2 个人查询
 - 22.2 Internet/Intranet流量统计计费系统
 - 22.3 计费系统主机的位置
 - 22.4 AllinOne服务器
 - 22.5 本章小结
- 第二十三章 数据库系统的安全性。
 - 23.1 数据库安全性要求
 - 23.2 数据库的完整性
 - 23.3 元素的完整性
 - 23.4 可审计性
 - 23.5 访问控制
 - 23.6 用户认证
 - 23.7 可获性
 - 23.7.1 访问判决
 - 23.7.2 间接攻击
 - 23.7.3 对统计推理攻击的控制
 - 23.8 本章小结
- 第二十四章 SQL服务器的安全性
 - 24.1 管理用户帐户
 - 24.1.1 数据库访问介绍
 - 24.1.2 SQL服务器登录标识符
 - 24.1.3 数据库用户
 - 24.1.4 数据库用户别名
 - 24.1.5 数据库组
 - 24.2 登录安全模式介绍
 - 24.2.1 标准安全模式
 - 24.2.2 集成安全模式
 - 24.2.3 混合安全模式
 - 24.3 用户许可简介
 - 24.3.1 语句许可与对象许可
 - 24.3.2 许可等级
 - 24.4 本章小结
- 第二十五章 Oracle的安全性
 - 25.1 Oracle安全性概述
 - 25.2 安全管理方法

- 25.2.1 用户名及口令的建立
- 25.2.2 用户名及口令的撤消
- 25.2.3 自动注册
- 25.2.4 Oracle用户的权限
- 25.2.5 授权及收回
- 25.2.6 授予和收回对数据库的存取权限
- 25.3 数据库的并发控制
 - 25.3.1 事务
 - 25.3.2 并发控制
 - 25.3.3 死锁问题的处理
- 25.4 本章小结
- 第二十六章 高可用性技术
 - 26.1 HA系统产生的背景
 - 26.2 HA系统体系结构比较
 - 26.2.1 双机硬盘镜像
 - 26.2.2 双机分布式硬盘镜像
 - 26.2.3 双机一双端口磁盘阵列
 - 26.3 双机一双端口磁盘阵列HA系统的实现
 - 26.4 磁盘阵列
 - 26.4.1 概述
 - 26.4.2 各种RAID级别介绍
 - 26.5 现有的高可用性解决方案
 - 26.6 高可用性产品
 - 26.7 本章小结
- 第二十七章 LotusNotes和Internet/Intranet
 - 27.1 Domino的Internet特性
 - 27.1.1 Domino基层结构
 - 27.1.2 使用Domino创建交互式Web站点
 - 27.1.3 创建Web站点的工具。
 - 27.1.4 使用Domino建立新闻组
 - 27.2 Domino和Intranet
 - 27.3 本章小结
- 第二十八章 Notes系统的安全性
 - 28.1 Domino系统的安全性
 - 28.1.1 防火墙
 - 28.1.2 加密
 - 28.1.3 Internet活动追踪
 - 28.1.4 Notes客户机
 - 28.2 网络安全性
 - 28.2.1 禁止未授权访问
 - 28.2.2 防止病毒
 - 28.2.3 保护物理系统
 - 28.3 层次结构名称.
 - 28.4 Domino服务器安全性
 - 28.5 Web浏览器安全性
 - 28.6 Notes客户机安全性

28.7 数据库安全性

28.7.1 存取级别

28.7.2 执行权限

28.7.3 角色

28.8 数据库加密

28.9 控制存取数据库设计元素

28.10 邮件安全性

28.11 本章小结

第二十九章 政务电子办公信息系统

29.1 信息管理系统结构设计

29.2 信息管理系统功能组件介绍

29.3 本章小结

第三十章 ExchangeServer及其安全性

30.1 MicrosoftExchange的层次结构

30.1.1 与WindowsNTServer的集成

30.1.2 客户机和服务器之间的通信

30.2 服务器体系结构

30.3 核心组件

30.3.1 目录

30.3.2 信息仓库

30.3.3 邮件传输代理

30.3.4 系统服务程序

30.4 可选组件

30.5 客户机体系结构

30.5.1 Schedule+

30.5.2 表单设计程序

30.5.3 可选的信息服务

30.6 服务器的高级安全保护

30.6.1 高级安全保护工作原理

30.6.2 密钥管理服务器

30.7 数字签名

30.7.1 邮件签名

30.7.2 加密邮件

30.7.3 解密邮件

30.7.4 选择加密类型

30.8 增加MicrosoftExchangeServer安全保护

30.8.1 改变在服务器安装过程中创建的共享目录的权限

30.8.2 配置加密RPC

30.9 保护Internet连接

30.9.1 配置Internet邮件连接器

30.9.2 保护用户帐号

30.9.3 使用WindowsNT文件系统

30.9.4 使用和配置服务

30.9.5 使用Internet邮件连接器连接到sMTP主机

30.9.6 使用Internet连接站点

30.9.7 DNS

30.10 允许客户在Internet上安全地连接.

- 30.10.1 指定宿主服务器
- 30.10.2 配置由宿主服务器域验证
- 30.10.3 配置防火墙允许RPC通信
- 30.11 本章小结
- 第三十一章 报表编辑和数据填充系统
- 31.1 概述
- 31.2 通信机制
- 31.3 软件组成和功能
- 31.3.1 报表查询子系统
- 31.3.2 报表设计子系统
- 31.3.3 Web报表上载系统
- 31.4 本章小结
- 第三十二章 综合应用实例
- 32.1 背景
- 32.2 需求分析
- 32.3 ACME组成、功能与结构
- 32.3.1 ACME的组成
- 32.3.2 系统结构
- 32.3.3 功能要求
- 32.4 系统物理配置
- 32.4.1 网络连接设备配置。
- 32.4.2 Internet和信息服务设备配置
- 32.4.3 OA和系统化业务支持设备配置
- 32.4.4 应用开发设备配置
- 32.4.5 网络/电话综合线系统
- 32.6 某开发区节点配置
- 32.5 安全考虑
- 32.5.1 攻击入口
- 32.5.2 安全构件的设置
- 32.6 本章小结
- 附录A 内容安全工具 MIMesWeeper
- 附录B 扫描工具
- 附录C 网络监听工具
- 附录D 检测和分析工具
- 附录E 网络访问控制验证工具
- 附录F 一些防火墙产品
- 附录G 一些邮件安全工具

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>