

<<局域网组建、维护与安全监控实战详解>>

图书基本信息

书名：<<局域网组建、维护与安全监控实战详解>>

13位ISBN编号：9787115214287

10位ISBN编号：711521428X

出版时间：2010-1

出版时间：刘晶、公芳亮 人民邮电出版社 (2010-01出版)

作者：刘晶，公芳亮 著

页数：339

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>

## 前言

随着网络的发展，网络互连的范围在不断地扩大。

局域网的复杂程度也由于网络应用的增加，在快速加大，使每一个网络工程师所要承担的责任和面临的风险也越来越大。

如何使用最简单、最快捷的方式管理局域网成为每一个网络工程师必需研究的方向。

作者作为大型网络服务器维护人员，长期从事几百台服务器的维护任务，对此深有体会。

本书的目的就是为了帮助网络工程师更好地搭建、设置和维护好局域网，提升读者的实战技能。

本书优势1.内容全面，突出安全本书完整地讲解局域网管理的各个环节，内容涉及网络构建、服务搭建、网络监控和网络安全实施。

内容深入浅出、连贯有序，使读者对整个局域网管理工作有一个整体认识。

2.实例讲解，贴近实战本书避免同类图书的大篇理论讲解，而是介绍大量的实际应用案例，并结合简单易懂的图例，让读者更容易理解网络的构成和管理。

3.重点突出，监控为主本书的内容重点是网络监控。

在网络管理工作中，大家重视网络搭建，忽视网络监控，从而造成局域网内病毒、木马泛滥。

本书着眼实际，详细讲解网络监控。

内容涉及Sniffer、Cacti、Nagios等专业软件的应用。

本书的组织结构本书共分为4篇。

第一篇为构建篇，包括第1~3章。

第1章帮助读者了解网络的基础，认识Internet；第2章讲解网络的构成；第3章讲解局域网的搭建。

第二篇为服务搭建篇，包括第4~8章。

该篇内容按照标准的安装步骤搭建了Windows平台和Linux平台下的网络监控环境，并针对其常见的问题给出了解决方案。

## 内容概要

随着局域网应用的普及，局域网维护和安全成为一个热门议题。

《局域网组建、维护与安全监控实战详解》由浅入深，循序渐进地教给读者如何构建、维护局域网以及各类服务器的安全设置。

全书内容包括4篇，第一篇讲解网络的构成和搭建；第二篇讲解DHCP、共享服务、FTP、Web服务、数据库的搭建和安全防护；第三篇讲解网络设备监控、数据捕获、安全检测和网络故障判断与处理；第四篇讲解木马分析、检测和处理，单机安全策略实施，杀毒软件和防火墙应用。

《局域网组建、维护与安全监控实战详解》适合广大网络维护人员、网站管理人员和大专院校学生阅读。

## 作者简介

刘晶，主要研究方向为软件工程和网络工程，曾在趋势科技公司工作，参与研发基于风险控制及多层次管理CMAST的产品，现在燕山大学任职、参与“基于并行计算的神经网络物流智能预测系统的研究”、“优化AES算法对会计信息安全的研究”、“基于数据挖掘的河北省高校突发事件预警及辅助决策系统研究”等。

公芳亮，从事网络工作多年，具有大规模网络管理经验，对网络管理、监控有很好的研究。

曾参与千橡集团网络集群管理工作。

现就职于某网络公司。

## 书籍目录

第一篇 构建篇第1章 网络概述1.1 计算机网络的定义和功能1.1.1 计算机网络的定义1.1.2 计算机网络的功  
能1.2 计算机网络的组成1.2.1 硬件设备1.2.2 软件组件1.3 计算机网络的分类1.3.1 按覆盖范围分类1.3.2 按  
数据组织方式分类1.4 认识Internet1.4.1 常用Internet的协议简介1.4.2 Internet物理网的构成1.4.3 认识IP地  
址第2章 网络的构成2.1 OSI参考模型2.1.1 OSI模型构成2.1.2 OSI工作方式2.1.3 OSI数据处理2.2 网络协  
议2.2.1 NetBEUI协议2.2.2 IPX/SPX协议2.2.3 TCP/IP2.2.4 IPv6协议2.3 集线器Hub2.3.1 共享型2.3.2 IP广  
播2.3.3 单位时间2.4 交换机2.4.1 交换机工作原理2.4.2 交换机交换方式2.5 桥接2.5.1 桥接的功能实现及应  
用2.5.2 桥接器的分类和特点2.6 网卡2.6.1 网卡的基本工作信息2.6.2 MAC地址的产生2.7 网桥2.7.1 网桥的  
基本工作信息2.7.2 网桥的基本分类2.8 网关2.8.1 协议网关2.8.2 应用网关和安全网关2.9 路由器2.9.1 路由  
器的基本使用方法2.9.2 多路由协调方式2.9.3 路由的协议2.9.4 路由的算法2.10 路由器和网桥的比较2.11  
VLAN知识简介第3章 局域网络搭建3.1 Modem接入3.1.1 Modem概述3.1.2 拨号网络的使用3.2 ISDN接  
入3.2.1 认识ISDN3.2.2 ISDN终端设备3.2.3 ISDN的应用3.3 ADSL接入3.3.1 了解ADSL3.3.2 ADSL设备及安  
装3.3.3 ADSL的应用3.4 DDN接入3.4.1 了解DDN3.4.2 DDN业务种类3.4.3 DDN的接入方式3.5 Cable  
Modem接入3.5.1 了解Cable Modem3.5.2 Cable Modem设备3.5.3 Cable Modem接入方式的应用3.5.4 通  
过Cable Modem上网3.6 无线接入3.6.1 了解无线接入3.6.2 无线接入的应用3.6.3 实现无线上网3.7 局域网  
安全概述3.7.1 网络分段3.7.2 交换式集线器代替共享式集线器3.7.3 VLAN的划分3.8 VPN远程接入解决方  
案3.8.1 VPN设计原则3.8.2 LinuxVPN设计第二篇 服务搭建篇第4章 DHCP服务的搭建、配置与管理4.1  
DHCP服务基础4.1.1 DHCP的基本概念4.1.2 DHCP常用术语4.1.3 DHCP服务控制台4.2 搭建DHCP服  
务4.3 DHCP服务端的设置4.3.1 在DHCP服务器中添加作用域4.3.2 设置网关和DNS服务器4.3.3 捆绑IP地  
址和MAC地址4.3.4 跨子网使用DHCP服务器4.3.5 超级作用域的建立4.3.6 DHCP服务器测试4.4 DHCP服  
务器的安全管理4.4.1 启用DHCP审核记录4.4.2 指定DHCP管理用户第5章 共享服务5.1 文件共享服务搭  
建与安全管理5.1.1 设置文件共享5.1.2 设置共享文件夹的使用权限5.1.3 停止共享文件夹5.1.4 映射网络驱  
动器5.1.5 Guest账户使用5.1.6 设置共享文件夹用户权限策略5.2 打印共享服务搭建与安全管理5.2.1 安装  
网络打印机5.2.2 设置网络打印机5.2.3 共享打印机的客户端使用5.3 网络共享服务搭建与安全管理5.3.1  
服务器端设置5.3.2 网络客户端设置5.3.3 Windows2003的网络监视器的使用5.4 主机使用代理服务软  
件5.4.1 使用WinGate5.4.2 使用SYGate第6章 FTP服务器的搭建与安全设置6.1 架设FTP服务器基础6.1.1 预  
备知识6.1.2 架设FTP服务器流程6.2 配置IIS的FTP服务器环境6.2.1 安装FTP服务器组件6.2.2 取消匿名访  
问功能6.2.3 启用日志记录6.2.4 设置用户权限6.2.5 限制用户使用的空间6.2.6 限制访问的IP6.2.7 设置组策  
略6.3 创建IIS的FTP服务器6.3.1 使用FTP站点创建向导创建FTP站点6.3.2 从文件建立FTP站点6.3.3 创建虚  
拟目录6.3.4 设置查看连接用户6.3.5 设定FTP站消息6.3.6 配置匿名登录6.3.7 修改主目录文件夹6.3.8 配  
置FTP服务器的安全访问6.3.9 测试所建立的FTP服务器6.3.10 配置FTP日志设置6.4 使用Serv-U架设FTP  
服务器6.4.1 建立Serv-U服务器6.4.2 配置FTP服务器6.4.3 账户管理6.5 Linux下FTP服务器6.5.1 Linux下FTP  
服务器的安装6.5.2 linux下FTP服务器的配置6.5.3 配置MySQL验证6.5.4 测试pureFTP6.5.5 pureFTP的管理  
第7章 Web服务器的搭建与安全防护7.1 ASP服务器7.1.1 安装MicrosoftInternet信息服务7.1.2 配置匿名身  
份验证7.1.3 配置计数器及日志报警7.2 建立Web站点和虚拟目录7.2.1 配置IIS站点7.2.2 配置ASP服务  
器7.2.3 更改服务器主目录7.3 Apache服务器7.3.1 Apache服务器在Linux下的安装7.3.2 Linux下PHP的安  
装7.3.3 Apache服务器在Linux下的基本设置7.3.4 Apache服务器在Windows下的安装7.3.5 Apache服务器  
在Windows下的设置第8章 数据库的安装与安全防护8.1 Access安装与安全设置8.1.1 Access安装8.1.2  
Access的安全设置8.2 SQLServer安装与安全设置8.2.1 硬件和操作系统要求8.2.2 安装过程8.3 MySQL的安  
装与管理8.3.1 MySQL数据库的安装8.3.2 使用phpMyAdmin管理MySQL数据库第三篇 监控篇第9章 局域  
网数据监控的准备9.1 局域网数据捕获原理9.2 简单的主动监控例子9.2.1 安装PcAnywhere9.2.2 配置被控  
端主机9.2.3 建立主控主机连接9.2.4 远程登录Windows20009.3 安装Sniffer Pro9.3.1 Sniffer Pro的安装环  
境9.3.2 安装Sniffer Pro9.3.3 Sniffer捕获工作流程第10章 网络设备监控10.1 SNMP基本知识10.1.1 认  
识SNMP10.1.2 SNMP在Linux系统下的安装10.1.3 SNMP在Windows系统下的安装10.2 使用MRTG进行监  
控10.2.1 检查软件包安装情况10.2.2 Linux被监控主机配置SNMP服务10.2.3 Windows被监控主机配  
置SNMP服务10.2.4 安装配置MRTG10.3 使用Cacti进行监控10.3.1 Cacti安装环境配置10.3.2 建立Cacti数据

库10.3.3 安装rrdtools10.3.4 安装Cacti10.3.5 Linux被监控端SNMP设置10.3.6 Windows被监控端SNMP设置10.3.7 Cacti的设置10.4 使用Nagios进行监控10.4.1 Nagios监控主机程序的安装10.4.2 Nagios-plugins的安装10.4.3 被动监控模块nrpe的安装10.4.4 被动监控模块nrpe在Linux平台被监控机上的安装10.4.5 被动监控模块nrpe在Windows平台被监控机上的安装10.4.6 Nagios的配置10.4.7 使用Nagios主动监控被监控服务器10.4.8 使用Nagios被动监控被监控服务器第11章 网络数据捕获与监控11.1 主动捕获分析网络数据11.1.1 监控控制端的操作11.1.2 配合密码查看软件查看密码11.2 被动监听原理及基本协议分析11.2.1 分析地址解析协议(ARP)11.2.2 分析ICMP协议11.2.3 分析TCP协议11.2.4 分析UDP协议11.3 SnifferPro实际应用例子——捕获邮件信息11.3.1 了解密码传输方式11.3.2 定制过滤器11.3.3 捕获数据包11.3.4 获取密码11.3.5 邮件收发软件工作方式11.3.6 定制专用过滤器11.3.7 使用专用过滤器捕获数据包11.4 SnifferPro实际应用例子——捕获FTP信息11.4.1 FTP软件工作方式11.4.2 定制CuteFTP专用过滤器11.4.3 捕获及分析数据包11.5 Sniffer Pro实际应用例子——捕获MSN信息11.5.1 MSNMessenger通信工作方式11.5.2 定制MSN专用过滤器11.5.3 捕获数据包11.5.4 分析聊天信息第12章 安全检测12.1 局域网的漏洞扫描12.1.1 常见网络漏洞12.1.2 使用SnifferPro检查网络漏洞12.2 使用工具进行网络扫描12.3 局域网的病毒监测12.3.1 监测网络情况12.3.2 制定病毒捕获措施12.3.3 特定病毒捕获实例第13章 常见网络故障判断与处理13.1 使用Cacti建立网络监控体系13.1.1 使用Cacti监控网络服务器CPU、硬盘和内存信息13.1.2 使用Cacti监控网络服务器网络流量13.1.3 使用Cacti监控网络服务13.1.4 使用Cacti的thold插件作全局监控13.2 使用SnifferPro判断网络问题13.2.1 分析原因13.2.2 简单案例分析第四篇 安全实施篇第14章 木马软件的分析、检测与处理14.1 木马概述14.1.1 木马类型14.1.2 特洛伊木马特性14.1.3 中木马后出现的状况14.1.4 木马常用端口14.2 使用Nagios建立木马监控体系14.2.1 使用Nagios监控木马程序端口14.2.2 使用Nagios邮件报警14.3 使用SnifferPro监控局域网内木马程序14.3.1 定制过滤器14.3.2 定制触发器第15章 单机安全设置15.1 单机安全概述15.2 安装设置杀毒软件15.2.1 安装瑞星个人防火墙15.2.2 瑞星杀毒软件的基本设置15.3 单机防火墙设置15.3.1 安装瑞星防火墙15.3.2 瑞星防火墙的基本设置15.3.3 瑞星防火墙的基本规则设置15.3.4 瑞星防火墙的基于端口规则设置15.3.5 瑞星防火墙的可信任区域的设置15.3.6 瑞星防火墙的IP规则设置15.3.7 瑞星防火墙的网站访问规则的设置第16章 集中式杀毒软件的部署和设置16.1 防病毒体系设计16.1.1 集中式防病毒体系的系统构架16.1.2 集中式防病毒体系的网络构架16.2 Symantec防病毒体系的安装16.2.1 Symantec病毒防护服务器的安装16.2.2 Symantec病毒防护服务器的基础设置16.2.3 Symantec病毒防护服务器的高级设置16.2.4 Symantec病毒防护服务器的网络16.2.4 设置及客户端网络安装第17章 防火墙解决方案17.1 网络防火墙概述17.1.1 防火墙的基本概念17.1.2 防火墙的优点和缺陷17.1.3 防火墙常见网络拓扑17.2 ISA防火墙的基本安装和设置17.2.1 ISA的服务器端安装17.2.2 ISA防火墙客户端的安装17.2.3 ISA防火墙的应用17.3 IPtables防火墙的基本安装和设置17.3.1 IPtables基础17.3.2 启动及IPtables使用范例

章节摘录

插图：1.管道网关管道是不兼容的网络区域传输数据的通用技术。

数据分组被封装在可以被传输网络识别的帧中，到达目的地时，接收主机解开封装，把封装信息丢弃，这样分组就被恢复到了原先的格式。

管道技术只能用于3层协议，从SNA到IPv6。

虽然管道技术有能够克服特定网络拓扑限制的优点，它也有缺点。

管道的本质可以隐藏不该接受的分组。

简单地说，管道可以通过封装来攻破防火墙，把本该过滤掉的数据传给私有的网络区域。

2.专用网关很多的专用网关能够在传统的大型机系统和迅速发展的分布式处理系统间建立桥梁。

典型的专用网关用于把基于PC的客户端连到局域网边缘的转换器。

该转换器通过X.25网络提供对大型机系统的访问。

3.2层协议网关2层协议网关提供局域网到局域网的转换。

它们通常被称为翻译网桥而不是协议网关。

在使用不同帧类型或时钟频率的局域网间互连可能就需要这种转换。

2.8.2应用网关和安全网关应用网关是在使用不同数据格式间翻译数据的系统。

典型的应用网关作用是接收一种格式的输入数据，将翻译，然后以新的数据格式发送。

输入和输出接口可以是分立的也可以使用同一网络连接。

一种应用可以有多种应用网关，如E-mail可以以多种格式实现，提供E-mail的服务器可能需要与各种格式的邮件服务器交互，实现此功能唯一的方法是支持多个网关接口。

应用网关也可以用于将局域网客户机与外部数据源相连，这种网关为本地主机提供了与远程交互式应用的连接。

将应用的逻辑和执行代码置于局域网中的客户端，避免了低带宽、高延迟的广域网的缺点，这就使得客户端的响应时间更短。

应用网关将请求发送给相应的计算机，获取数据，如果需要就把数据格式转换成客户机所要求的格式。

安全网关是各种技术有趣的融合，具有重要且独特的保护作用，其范围从协议级过滤到十分复杂的应用级过滤。

编辑推荐

《局域网组建、维护与安全监控实战详解》有15个网络管理和安全监控案例：局域网、DHCP服务的搭建、Windows和Linux平台下FTP服务器、Web服务器、数据库的管理与安全防护，局域网数据监控，局域网漏洞扫描，常见网络故障，网络设备监控，网络数据捕获与监控，共享服务，木马的检测与防范，单机安全设置，集中式杀毒软件的部署，防火墙解决方案。涵盖Windows和Linux两大平台，讲解5大软件Sniffer、MRTG、Cacti、Nagios、PcAnywhere的使用从组建、维护到安全监控，全实例呈现网络管理技术



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>