

<<新编网络安全教程>>

图书基本信息

书名：<<新编网络安全教程>>

13位ISBN编号：9787030152954

10位ISBN编号：7030152956

出版时间：2005-6

出版时间：科学出版社

作者：中科希望技术培训学校

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>

## 书籍目录

第1章 网络安全基础知识1.1 入侵范式剖析1.1.1 入侵范式介绍1.1.2 入侵范式事例1.2 认识攻击者1.2.1 入侵动机1.2.2 攻击者分类1.3 网络安全目标1.3.1 隐私性保护1.3.2 数据完整性保护1.3.3 用户身份认证1.3.4 网络可用性保护1.4 TCP/IP网络1.4.1 TCP/IP协议模型1.4.2 IP地址1.4.3 子网掩码1.4.4 IP地址扩展技术1.4.5 TCP/IP协议报文结构1.4.6 TCP连接过程1.4.7 DNS和网络安全1.5 路由技术1.5.1 路由器1.5.2 路由器的防火墙功能1.5.3 路由表1.5.4 路由协议1.6 工作站安全防护1.6.1 加固工作站的基本原则1.6.2 建立工作站的资源考虑1.6.3 保护Windows 2000以及XP计算机1.6.4 保护UNIX以及Linux计算机1.7 本章小结第2章 网络防护设计2.1 常见攻击及威胁2.1.1 网络漏洞2.1.2 拒绝服务攻击(DoS)2.1.3 中间人攻击(Man-in-the-Middle)2.1.4 缓冲区溢出攻击2.1.5 网络嗅探攻击2.2 网络防护层次2.2.1 物理安全2.2.2 密码安全2.2.3 操作系统安全2.2.4 反病毒防护2.2.5 包过滤2.2.6 防火墙2.2.7 代理服务器2.2.8 DMZ(非军事区)2.2.9 入侵检测系统2.2.10 虚拟专用网(VPN)2.2.11 日志和管理2.3 网络安全操作2.3.1 访问控制2.3.2 加密2.3.3 认证2.3.4 开发包过滤规则库2.3.5 病毒检测2.3.6 远程安全访问2.3.7 日志文件处理2.4 集成入侵检测系统2.4.1 攻击预测2.4.2 IDS通告选项2.4.3 部署IDS2.4.4 入侵检测的报警响应2.5 本章小结第3章 风险分析和安全策略设计3.1 风险分析3.1.1 风险分析的基本概念3.1.2 风险分析方法3.1.3 风险分析计算3.1.4 成本影响分析3.2 风险最小化3.2.1 硬件保护3.2.2 保护等级排序3.2.3 信息保护3.2.4 定期进行风险分析3.2.5 制定安全事件响应程序3.3 制定安全策略3.3.1 如何制定好的安全策略3.3.2 制定安全策略的步骤3.3.3 安全策略的分类3.3.4 在Windows Server 2003下制定安全策略3.4 本章小结第4章 选择和设计防火墙4.1 选择堡垒主机4.1.1 一般性要求4.1.2 选择主机4.1.3 明确堡垒主机的职能4.1.4 备份和审计4.2 防火墙及体系结构4.2.1 防火墙是什么4.2.2 屏蔽路由器结构4.2.3 宿主主机结构4.2.4 主机过滤结构4.2.5 子网过滤结构4.2.6 多重防火墙结构4.2.7 反向防火墙4.3 防火墙的功能4.3.1 包过滤功能4.3.2 网络地址转换4.3.3 代理服务功能4.3.4 加密身份认证4.3.5 加密隧道4.3.6 Windows 2000的防火墙功能4.4 选择防火墙4.4.1 选择防火墙的基本原则4.4.2 软件防火墙4.4.3 硬件防火墙4.4.4 混合防火墙4.5 建立防火墙规则和限制4.5.1 保持规则库的简洁性4.5.2 基于安全策略建立规则库4.5.3 建立应用程序规则4.5.4 限制或允许子网规则4.5.5 控制Internet服务4.6 本章小结第5章 配置防火墙5.1 包过滤的方法5.1.1 无状态的包过滤5.1.2 有状态的包过滤5.1.3 包过滤功能对部署位置的依赖性5.2 创建包过滤规则5.3 网络地址转换5.3.1 NAT技术的定义5.3.2 NAT的类型5.3.3 NAT技术的安全问题5.4 用户认证5.4.1 确定认证类型5.4.2 认证信息5.4.3 组合认证方法5.5 本章小结第6章 管理和使用防火墙6.1 防火墙与代理服务器6.1.1 代理服务器的功能6.1.2 代理服务器的工作原理6.1.3 选择代理服务器6.1.4 内容过滤6.2 管理防火墙6.2.1 校订规则库6.2.2 管理日志文件6.2.3 提高防火墙性能6.2.4 配置高级防火墙功能6.3 Microsoft ISA Server 2004防火墙6.3.1 安装6.3.2 配置网络6.3.3 配置网络规则6.3.4 防火墙策略6.3.5 入侵检测功能6.4 IPTables防火墙6.4.1 安装和启动防火墙6.4.2 Netfilter防火墙系统框架6.4.3 Netfilter防火墙在IPv4中实现原理和结构6.4.4 建立规则和链6.4.5 防火墙实例6.4.6 nctfiltcr/iptables系统的优点6.5 本章小结第7章 建立虚拟专用网7.1 VPN技术简介7.1.1 什么是VPN7.1.2 为何建立VPN网络7.1.3 VPN网络配置7.2 隧道协议7.2.1 PPTP7.2.2 L2F7.2.3 L2TP7.2.4 IPSec7.2.5 SOCKs V.57.2.6 SSH7.3 VPN的加密方案7.3.1 DES算法7.3.2 3DES算法7.3.3 SSL7.3.4 Krcbcros7.4 VPN的过滤规则7.4.1 PPTP筛选器7.4.2 L2TP和IPSec筛选器7.5 本章小结第8章 入侵检测系统8.1 入侵检测的分类8.1.1 入侵检测技术8.1.2 入侵检测的数据来源8.1.3 入侵检测方式8.2 入侵检测技术8.2.1 异常入侵检测技术8.2.2 基于特征的入侵检测8.2.3 智能入侵检测技术8.3 入侵检测系统模型8.3.1 通用入侵检测模型8.3.2 通用入侵检测框架8.3.3 IDWG工作组8.4 入侵检测系统组件8.4.1 网络传感器8.4.2 报警系统8.4.3 命令控制台8.4.4 响应系统8.4.5 攻击特征数据库8.5 入侵检测的过程8.6 入侵检测系统8.6.1 主机入侵检测系统8.6.2 网络入侵检测系统8.6.3 混合入侵检测系统8.7 入侵检测系统评估8.7.1 免费入侵检测系统8.7.2 基于主机的入侵检测系统8.7.3 基于网络的入侵检测系统8.7.4 异常入侵检测系统8.7.5 特征入侵检测系统8.7.6 IDS硬件设备8.8 Snort网络入侵检测系统8.8.1 Snort简介8.8.2 安装Snort8.8.3 Snort运行方式8.8.4 编写snort规则8.9 本章小结第9章 计算机犯罪与计算机取证9.1 计算机犯罪案件的概述9.1.1 计算机犯罪的类型、特点及原因9.1.2 计算机犯罪的现状和发展趋势9.2 计算机犯罪案件的侦查条件9.2.1 计算机犯罪案件侦查技术上的依托9.2.2 计算机犯罪案件侦查法律上的保障9.2.3 侦查人员素质的提高9.3 计算机犯罪案件的侦查过程9.3.1 计算机犯罪的线索来源9.3.2 计算机犯罪案件的技术侦查途径9.3.3 电子证据的获

取9.4 计算机取证9.4.1 计算机取证的历史及现状9.4.2 计算机取证的定义9.4.3 计算机取证步骤9.4.4 计算机证据恢复及获取技术9.4.5 计算机证据的保全技术9.4.6 计算机取证工具9.5 一个计算机案件取证过程的完整实例9.5.1 日志文件分析9.5.2 恢复的删除文件分析9.6 本章小结第10章 Windows系统安全应用10.1 使用账户密码策略保证计算机安全10.2 使用账户锁定策略保证计算机安全10.3 设置Windows Server2003的审核策略10.4 设置Windows的用户权限分配策略以保证系统安全10.5 设置Windows的安全选项以保证系统安全10.6 本章小结附录A Keberos协议

## <<新编网络安全教程>>

### 编辑推荐

本书主要介绍了网络安全和防护方面最重要的概念及相关知识。通过本教程的学习，读者将具备必要的网络安全知识，并且能够利用这些基础知识和相应的安全防护工具，比如防火墙、入侵检测系统等，提供的安全措施对系统进行安全保护。

全书分为10章，内容包括：网络安全基础知识，网络防护设计，风险分析和安全策略设计，选择和设计防火墙，配置防火墙，加可是和管理防火墙，虚拟专用网（VPN），入侵检测系统，计算机犯罪及计算机取证以及Windows系统安全应用等。

本书内容新颖全面，是系统安全工程师、网络安全管理员和信息系统工程以及有志于从事系统和网络安全管理的工程人员的首选书籍。

<<新编网络安全教程>>

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>