<<企业网络整体安全>>

图书基本信息

书名：<<企业网络整体安全>>

13位ISBN编号：9787121133701

10位ISBN编号：7121133709

出版时间：2011-8

出版时间：电子工业

作者：谌玺

页数：410

<<企业网络整体安全>>

内容概要

本书深入地剖析了构成企业网络整体安全的各部分，包括网络安全概述、网络设备的工作原理、设备造成的安全威胁、各种开放式网络协议，以及开放式网络协议所造成的安全威胁、基于网络设计及网络架构的攻击与防御技术、路由协议的工作原理与攻击防御技术、网络设备的加固技术与检测方法、防火墙的配置、病毒与木马的检测与防御、网络集中验证、访问控制与接入端口的安全技术等。由浅入深，论点有据，将不可见的理论变成形象的数据帧，并经过有序的组织，让读者结束对理论的理想型学习方式，让理论更好理解，可阅读性更强。

本书还讲述了现今最流行的与网络安全密切相关的流量分析技术、流量渗透分析与防御技术、在受到网络攻击时服务质量保证技术、网络安全评估技术、网络安全的加固技术等。
大篇幅地揭露了防火墙与杀毒软件视而不见的高危险性攻击与入侵方式、演示防御措施等。
本书将附赠教学与实验光盘，使读者感受视听相结合的学习方式，更加形象，更易入手。

<<企业网络整体安全>>

书籍目录

第1章 网络安全概述
1.1 什么是网络安全
1.2 典型的网络安全违例事件
1.3 引发网络安全违例行为（事件）的途径
1.4 企业级网络安全的实现指南
1.4.1 网络安全意识
1.4.2 初期网络建设就应该考虑安全
1.4.3 网络安全管理条例
1.4.4 网络安全评估
1.4.5 安全加固
1.4.6 安全联动
1.5 网络安全的范围
1.5.1 资产安全
1.5.2 风险分析
1.5.3 数据安全
1.5.4 数据存储和恢复安全
1.5.5 数据传输安全
1.5.6 数据访问权限安全
1.5.7 移动存储设备管理
1.5.8 网络安全运行应急预案
1.5.9 网络架构安全
1.5.10 威胁确定
1.5.11 策略制订与安全加固
1.5.12 安全应急预案
1.6 分析：黑客入侵的过程
1.6.1 扫描
1.6.2 确定攻击或入侵对象
1.6.3 检查对象漏洞
1.6.4 分析：黑客的入侵攻击
1.7 小结
第2章 网络设备的工作原理与安全威胁
2.1 集线器的工作原理与安全威胁
2.2 演示：集线器的入侵与防御
2.3 网桥、二层交换机的工作原理与安全威胁
2.4 演示：网桥、二层交换机的入侵与防御
2.5 路由器的工作原理与安全威胁
2.6 演示：路由器的入侵与防御
2.7 防火墙的工作原理与安全威胁
2.8 小结
第3章 渗透分析开放式网络协议
3.1 为什么要分析开放式协议
3.1.1 分析开放式协议的难度
3.1.2 利用什么工具分析开放式协议
3.1.3 理解Sniffer_pro的使用
3.2 利用协议分析器分析开放式协议

3.2.1 利用协议分析器分析ARP的工作原理
3.2.2 利用协议分析器分析TCP/IP的工作原理
3.2.3 利用协议分析器分析ICMP的工作原理
3.2.4 利用协议分析器分析DHCP的工作原理
3.2.5 利用协议分析器分析DNS的工作原理
3.2.6 利用协议分析器分析主动FTP与被动FTP的工作原理
3.2.7 利用协议分析器分析Telnet和SSH的工作原理
3.2.8 利用协议分析器分析HTTP的工作原理
3.3 小结
第4章 开放式协议的攻击与防御
4.1 演示ARP攻击与ARP攻击的防御
4.2 演示TCP/IP攻击与防御
4.3 演示基于ICMP的攻击与防御
4.4 演示：DHCP攻击与防御
4.5 演示：DNS的攻击与防御
4.6 演示：FTP的攻击与防御
4.7 演示：UDP攻击与防御
4.8 小结
第5章 理解基于网络结构的攻击与防御
5.1 基于数据链路层的攻击与防御
5.1.1 分析与取证：生成树协议（STP）技术的工作原理
5.1.2 演示：基于STP技术的攻击与防御
5.1.3 分析与取证：思科邻居发现协议（CDP）的工作原理
5.1.4 演示：基于CDP技术的攻击与防御
5.1.5 分析与取证：VLAN的工作原理与通信过程
5.1.6 演示：基于VLAN的双标记攻击
5.2 基于网络层的攻击与防御
5.2.1 路由的基本原理与实现
5.2.2 演示：RIP路由协议的工作原理与实现
5.2.3 演示：基于动态路由协议RIP的入侵与防御
5.2.4 思科HSRP的工作原理与实现
5.2.5 演示：基于思科的HSRP攻击与防御
5.3 小结
第6章 网络安全流量检测与QoS技术
6.1 流量统计与分析
6.1.1 利用Sniffer统计与分析流量
6.1.2 利用NetFlow统计与分析流量
6.1.3 利用NBAR统计与分析流量
6.2 QoS技术入门
6.2.1 详解IP报文的优先级字段
6.2.2 理解QoS的策略过程
6.2.3 演示：IP报文的标记
6.3 理解QoS队列技术
6.3.1 理解FIFOQ、WFQ、CBWFQ和LLQ
6.3.2 演示：使用基于类别的队列（CBWFQ）技术控制企业网络的流程工程
6.3.3 演示：使用低延迟队列（LLQ）保证企业语音及视频会议流量
6.3.4 理解限速器CAR的工作原理

6.3.5 演示：利用CAR缓解ICMP攻击
6.4 企业级网络流量管理的经典案例演示
6.4.1 演示：利用NBAR技术完成对典型的网络病毒进行审计并过滤
6.4.2 演示：利用NBAR防止泛滥下载MP3、大型的视频文件、图片文件
6.4.3 演示：针对P2P流量控制的解决方案
6.5 小结
第7章 Windows操作系统的安全加固
7.1 理解Windows服务器基本的安全特性
7.1.1 操作系统的登录验证
7.1.2 配置操作系统的SysKey
7.1.3 操作系统的用户与权限
7.1.4 操作系统控制资源访问
7.1.5 加密文件系统
7.1.6 夺取Windows操作系统的文件拥有者权限
7.1.7 演示：暴力破解Windows安全账户管理器
7.2 操作系统面对的安全威胁
7.2.1 木马与病毒对操作系统造成的威胁
7.2.2 演示：灰鸽子木马的制作、隐藏、传播及防御
7.2.3 演示：微软RPC的冲击波蠕虫病毒的入侵与防御
7.2.4 分析Auto病毒的传播原理与防御方式
7.2.5 针对Windows操作系统做TCP洪水攻击的防御
7.2.6 针对Windows 操作系统的ICMP洪水攻击与防御
7.3 针对Windows操作系统的加固措施
7.3.1 对Windows操作系统进行安全评估
7.3.2 集中部署Windows的补丁分发管理服务器
7.3.3 监控Windows的运行情况——利用性能监视器实时监控TCP洪水攻击
7.3.4 建立Windows的审核项目——审核用户对资源的访问
7.4 小结
第8章 灾难保护与备份
8.1 灾难保护范围
8.1.1 理解磁盘阵列
8.1.2 理解Windows操作系统的动态磁盘
8.1.3 理解Windows服务器的简单卷
8.1.4 理解Windows服务器的跨区与带区阵列
8.1.5 理解Windows服务器的镜像阵列
8.1.6 理解Windows服务器的RAID-5阵列
8.1.7 演示：基于Windows 系统的镜像阵列
8.1.8 演示：基于Windows 系统的RAID-5阵列
8.2 数据备份
8.2.1 灾难保护并不能替代数据备份
8.2.2 理解各种数据备份的方式
8.2.3 演示：制订安全的数据备份
8.2.4 演示：制订自动备份计划
8.2.5 数据备份不能替代实时备份
8.2.6 演示：使用UPM备特佳灾备系统完成数据的实时备份
8.3 小结
第9章 信息安全的集中管理

9.1 为企业网络建立统一的时钟系统
9.2 分析与取证：网络集中管理必备协议SNMP的工作原理
9.3 演示：使用SNMP协议完成企业网络设备的集中管理
9.4 理解在各种不同系统平台上的日志收集
9.5 演示：集中收集各种网络设备与服务器的日志文件
9.6 演示：对日志信息的解析与日志的过滤
9.7 演示：利用DHCP Snooping接合DAI技术智能防御网络中的ARP攻击
9.8 演示：快速控制企业级网络遭遇病毒后的交叉感染
9.9 演示：基于桌面系统的接入验证与控制
9.10 建立信息安全带外管理方案
9.11 加固企业网络的安全配置
9.11.1 企业级网络安全设备的种类与应用范围
9.11.2 配置思科的IOS防火墙
9.11.3 配置思科的PIX防火墙
9.11.4 配置思科基于IOS与PIX的入侵防御系统
9.11.5 利用SDM加固路由器与交换机的安全
9.12 小结
附录A 和本书有关的Ubuntu操作系统的使用基础
附录B P2P软件常用的端口号
附录C SDM的安装使用

媒体关注与评论

我国的信息安全建设已进入一个新的时代，在这个新的时代里，网络安全建设已经不再单纯地立足于安全产品、安全软件、病毒处理与木马防御，而是面向整体网络结构、网络设计，甚至于针对网络安全产品本身的加固与防御。

“能够被安全产品或杀毒软件检测出来的安全违规事件，将不再是问题。最大的问题是已经发生了，却没有被查出来的问题。”常规的写作是文献参考，成功的写作是将文献参考变为案例演示，伟大的写作是启发读者。“读之所欲！作之必从！”

——笔者

<<企业网络整体安全>>

编辑推荐

谌玺、张洋所著的《企业网络整体安全——攻防技术内幕大剖析(附光盘)》重点讲解安全产品无法抵御的攻击方式与入侵手段。

本书所有的知识点和攻击防御的演示过程都被制作成详细的演示录像，让读者在良好的视听环境下进行学习。

成功地将网络安全的深度理论与高端实验相结合。

提出了“基于网络结构与网络设计的安全威胁”的新概念，并且为不同企业的网络环境制订具有企业网络特色的安全防御案例。

版权说明