<<网络安全新技术>>

图书基本信息

书名：<<网络安全新技术>>

13位ISBN编号：9787115108227

10位ISBN编号：7115108226

出版时间：2003-1-1

出版时间：人民邮电出版社

作者：张千里,陈光英

页数：251

字数：396000

<<网络安全新技术>>

内容概要

网络安全是一门迅速发展的学科，随着网络攻击技术的发展，新的应对方法也不断涌现出来。
PDRR模型就是反映这种发展的一个全新理念和体系结构模型，在1988年莫里斯蠕虫事件之后，各种安全技术，尤其是入侵检测技术和紧急响应技术，得到了前所未有的发展。
它们正在整个网络安全体系结构中起着越来越大的作用。
　本书是一本介绍最新网络安全技术发展的书籍。
基于近年来提出的PDRR网络安全模型，本书分别介绍了安全防护、入侵检测、应急响应、系统恢复这四个方面在理论和实践中的最新发展。
　本书可供高等院校相关专业师生及网络安全从业人员阅读，对网络安全领域的研究人员和网络管理员也有一定的参考价值。

<<网络安全新技术>>

书籍目录

第1章 网络安全风险分析 1.1 网络协议缺陷 1.1.1 TCP/IP概述 1.1.2 TCP序列号预计 1.1.3 路由协议缺陷 1.1.4 网络监听 1.1.5 TCP/UDP应用层服务 1.2 软件实现缺陷 1.2.1 输入确认错误 1.2.2 访问确认错误 1.2.3 特殊条件错误 1.2.4 设计错误 1.2.5 配置错误 1.2.6 竞争条件错误 1.2.7 其他 缓冲区溢出 1.3 操作系统危险缺陷 1.3.1 公共缺陷检索（CVE，Common Vulnerabilities and Exposures） 1.3.2 UNIX操作系统最危险的缺陷 1.3.3 Windows操作系统最危险的缺陷 1.4 用户使用缺陷 1.4.1 易于破解的密码 1.4.2 软件使用错误 1.4.3 系统备份不完整 1.5 病毒与木马 1.5.1 计算机病毒 1.5.2 木马 1.5.3 恶意代码 1.6 本章小结 第2章 网络安全体系结构 2.1 信息安全总体框架 2.1.1 安全特性 2.1.2 系统单元 2.1.3 OSI参考模型 2.2 OSI 安全体系结构 2.2.1 安全服务 2.2.2 安全机制 2.2.3 安管理 2.3 PDRR网络安全模型 2.3.1 防护 2.3.2 检测 2.3.3 响应 2.3.4 恢复 2.4 本章小结第3章 系统安全防护 3.1 操作系统安全概述 3.1.1 操作系统安全概念 3.1.2 计算机操作系统安全评估 3.1.3 国内的安全操作系统评估 3.1.4 操作系统的安全配置 3.2 Windows系统安全防护 3.2.1 Windows 2000 操作系统安全性能简介 3.2.2 Windows 2000安全配置 3.3 UNIX/Linux系统安全防护 3.3.1 Solaris系统安全管理 3.3.2 Linux安全防护 3.4 常见服务的安全防护 3.4.1 WWW服务器的安全防护 3.4.2 Xinetd超级守护程序配置 3.4.3 SSH 3.5 本章小结第4章 网络安全防护 4.1 网络安全管理政策 4.1.1 鉴定网络连接的类型 4.1.2 审核网络特点和相关的信任关系 4.1.3 确定安全风险的类型 4.1.4 确定适当的潜在防护领域并建立防护措施 4.1.5 文字表述安全管理政策 4.2 网络安全风险评估 4.2.1 网络安全风险评估的主要概念 4.2.2 风险评估过程 4.2.3 评估方法的选择 4.3 网络访问控制和防火墙 4.3.1 访问控制简介 4.3.2 防火墙简介 4.3.3 防火墙的主要功能 4.4 本章小结 第5章 数据安全防护 5.1 数据存储安全 5.1.1 网络数据备份 5.1.2 网络备份系统 5.1.3 归档管理系统 5.1.4 系统容错技术 5.2 数据保密鉴别 5.2.1 对称加密方法 5.2.3 公开密钥加密方法 5.2.4 消息摘要函数 5.2.5 数字签名 5.2.6 数字证书 5.2.7 公钥基础设施（PKI） 5.3 数据通信安全 5.3.1 互联网模型应用保密和鉴别技术 5.3.2 端对端保密和鉴别通信 5.3.3 应用层加上数据保密和鉴别模块 5.3.4 安全插座层（SSL） 5.3.5 安全IP（IPSec） 5.4 本章小结第6章 入侵检测系统 6.1 入侵检测基本概念 6.1.1 什么是安全 6.1.2 什么是攻击、入侵 6.1.3 什么是入侵检测系统 6.1.4 为什么需要入侵检测系统 6.1.5 基于主机和基于网络的入侵检测系统 6.1.6 误用检测和异常检测 6.2 入侵检测技术分析 6.2.1 入侵检测原理 6.2.2 入侵检测系统统一模型 6.2.3 总体结构 6.2.4 目标 6.2.5 定时 6.2.6 信息收集器 6.2.7 分析器 6.2.8 响应选项 6.3 入侵检测效果的评测 6.3.1 测试数据源 6.3.2 检测错误 6.3.3 包装评测 6.4 入侵检测系统的未来 6.4.1 入侵检测系统有很大的市场前景 6.4.2 提高入侵检测的速度 6.4.3 硬件化 6.4.4 专业化 6.4.5 异常检测 6.4.6 人工智能的应用 6.4.7 互联化 6.4.8 标准化 6.4.9 与法律结合 6.4.10 蜜罐技术（Honey Pot） 6.5 本章小结第7章 紧急响应理论和实践 7.1 紧急响应的概念和历史 7.1.1 紧急响应的背景和基本概念 7.1.2 常见安全事件及处理 7.2 紧急响应小组的建立框架 7.2.1 CSIRT 框架 7.2.2 服务和质量 7.2.3 与特定的需要符合 7.3 事件处理 7.3.1 紧急响应的描述 7.3.2 紧急响应功能综述 7.3.3 分类的职能 7.3.4 事件处理功能 7.3.5 交流 7.3.6 信息处理 7.4 紧急响应小组的其他业务 7.4.1 公告 7.4.2 反馈 7.5 本章小结第8章 系统的恢复 8.1 系统恢复 8.1.1 切断被入侵系统的入侵者访问途径 8.1.2 复制一份被侵入系统 8.1.3 入侵途径分析 8.1.4 遗留物分析 8.1.5 检查网络上的其他系统和涉及到的远程站点 8.1.6 评估入侵事件的影响，重建系统 8.2 后门的检查和清除 8.2.1 什么是后门 8.2.2 常见的后门种类 8.2.3 常用的检测和清除工具软件 8.3 本章小结结束语--网络安全未来

<<网络安全新技术>>

版权说明