第一图书网, tushu007.com

# <<网络安全原理与应用>>

## 图书基本信息

书名：<<网络安全原理与应用>>

13位ISBN编号：9787121171901

10位ISBN编号：7121171902

出版时间：2012-6

出版时间：电子工业出版社

作者：陈志德，许力　主编

页数：344

字数：580000

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

本书主要系统地介绍了网球安全的基本原理和基本应用。
全书主要分理论篇和试验篇，共19章，主要包括引论、对称密码、公钥密码、安全协议、操作性也安全、多媒体信息安全、防火墙、入侵检测、病毒原理与防范、数据库安全技术、无限网络安全等网络安全原理，以及Windows
Server服务器安全配置试验、Web检测试验、密码试验、系统扫描试验、网络监控与嗅探试验、破译与攻击试验、防火墙试验和入侵检测试验等网络安全实验与应用。

## 书籍目录

第一篇 理 论 篇
第1章 引论
1.1 网络安全的基础
1.1.1 网络安全的含义
1.1.2 网络安全的特征
1.1.3 网络安全的目标
1.1.4 网络安全的体系结构
1.2 威胁网络安全的因素
1.2.1 网络的安全威胁的类型
1.2.2 物理设备脆弱性
1.2.3 软件系统脆弱性
1.2.4 协议实现的脆弱性
1.2.5 网络架构的脆弱性
1.2.6 经营和管理带来的脆弱性
1.3 网络安全的防御技术
1.3.1 数据加密
1.3.2 网络故障检测与安全评估
1.3.3 故障恢复与保护倒换
1.3.4 信息传输安全
1.3.5 互联网安全
1.3.6 网络欺骗技术与蜜罐技术
1.3.7 黑客追踪技术
1.4 信息网络安全策略和安全保护体系
1.4.1 信息网络安全策略
1.4.2 信息网络安全保护体系
1.5 计算机系统的安全标准
1.6 网络安全法律法规
1.6.1 国外网络安全相关法律法规
1.6.2 我国网络安全法制法规建设
第2章 对称密码
2.1 引言
2.2 古典密码
2.2.1 古典密码简介
2.2.2 代换密码
2.2.3 置换密码
2.3 分组密码
2.3.1 DES算法的描述
2.3.2 AES算法结构
2.3.3 其他分组密码
2.4 序列密码
2.4.1 线性反馈移位寄存器
2.4.2 非线性序列密码
2.4.3 RC4序列密码
第3章 公钥密码
3.1 公钥密码概述

3.2 RSA密码体制
3.2.1 简介
3.2.2 RSA密钥的产生
3.2.3 RSA的安全性分析
3.2 椭圆曲线密码体制
3.2.1 椭圆曲线
3.2.2 椭圆曲线上的密码
第4章 安全协议
4.1 密钥管理协议
4.1.1 Shamir门限方案
4.1.2 Diffie-Hellman密钥交换协议
4.2 IP层安全协议
4.2.1 IPSec安全体系结构
4.2.2 安全关联
4.2.3 SA的创建
4.2.4 SA的删除
4.2.5 安全策略数据库（SPD）
4.2.6 IPSec模式
4.2.7 IPSec处理
4.2.8 认证报头
4.2.9 AH报头格式
4.2.10 AH模式
4.2.11 AH处理
4.2.12 封装安全有效载荷
4.2.13 ISAKMP
4.3 Kerberos协议
4.3.1 Kerberos协议的结构
4.3.2 Kerberos交换
4.3.3 Kerberos票据标志
4.4 SSL协议
4.4.1 SSL协议的分层结构
4.4.2 SSL协议支持的密码算法
4.4.3 SSL协议的通信主体
4.4.4 SSL协议中的状态
4.4.5 SSL记录协议
4.4.6 改变密码规范协议
4.4.7 告警协议
4.4.8 握手协议
第5章 操作系统安全
5.1 操作系统安全概述
5.1.1 操作系统安全需求
5.1.2 安全策略
5.1.3 安全功能
5.1.4 安全模型
5.1.5 安全操作系统存在的问题
5.2 操作系统的硬件安全机制
5.2.1 内存保护

5.2.2 运行域保护
5.2.3 I/O保护
5.3 操作系统的软件安全机制
5.3.1 身份识别
5.3.2 访问控制技术
5.3.3 访问控制机制
5.4 安全操作系统漏洞扫描
5.5 操作系统安全审计
5.5.1 审计追踪
5.5.2 审计内容
5.6 操作系统安全测评
第6章 多媒体信息安全
6.1 多媒体信息安全概述
6.2 数字水印技术
6.2.1 数字水印技术概述
6.2.2 数字水印基本特征
6.2.3 数字水印的应用
6.2.4 数字水印分类
6.2.5 几种常见的水印算法
6.3 数字版权管理
6.3.1 概念
6.3.2 基本特点
6.3.3 基本原理
6.3.4 数字版权管理关键技术
6.3.5 DRM保护版权的步骤
第7章 防火墙
7.1 防火墙概述
7.1.1 防火墙的概念
7.1.2 防火墙的主要作用
7.1.3 防火墙的局限性
7.1.4 防火墙的类型
7.1.5 防火墙的发展趋势
7.2 防火墙技术
7.2.1 简单包过滤型
7.2.2 状态检测型
7.2.3 应用代理型
7.2.4 防火墙基本技术对比
7.2.5 防火墙技术实例
7.2.6 防火墙应用中的新技术
7.3 防火墙架构
7.3.1 屏蔽路由器
7.3.2 双宿主主机网关
7.3.3 被屏蔽主机网关
7.3.4 被屏蔽子网
7.4 防火墙的选购与配置
7.4.1 防火墙产品介绍
7.4.2 防火墙选购原则

7.4.3 防火墙设计策略
第8章 入侵检测
8.1 入侵检测概述
8.1.1 入侵检测的必要性
8.1.2 入侵检测的定义
8.1.3 入侵检测的历史
8.1.4 入侵检测的分类
8.1.5 入侵检测系统的体系结构
8.2 入侵检测技术
8.2.1 入侵检测的信息源
8.2.2 异常检测技术
8.2.3 误用检测技术
8.3 典型的入侵检测系统——Snort
8.3.1 入侵检测系统的概念系统与商业产品
8.3.2 Snort简介
8.3.3 Snort总体工作流程
8.3.4 Snort体系结构
8.3.5 Snort规则集
8.3.6 Snort的功能模块
8.4 入侵检测的发展
第9章 病毒原理与防范
9.1 计算机病毒概述
9.1.1 计算机病毒发展史
9.1.2 计算机病毒的定义和特征
9.1.3 计算机病毒的分类
9.1.4 计算机病毒的发展趋势
9.2 计算机病毒的基本原理
9.2.1 计算机病毒的基本结构
9.2.2 计算机病毒的磁盘存储结构
9.2.3 计算机病毒的内存驻留结构
9.2.4 计算机病毒的引导机制
9.2.5 计算机病毒的传染机制
9.2.6 计算机病毒的触发机制
9.2.7 计算机病毒的破坏机制
9.3 计算机病毒的防范
9.3.1 反病毒技术的发展历程
9.3.2 基于主机的检测策略
9.3.3 基于网络的检测策略
第10章 数据库安全技术
10.1 数据库安全概述
10.1.1 数据库的基本概念
10.1.2 数据库系统的特性
10.1.3 数据库安全的重要性
10.1.4 数据库系统面临的安全威胁
10.1.5 数据库的安全要求
10.2 数据库安全技术
10.2.1 数据库安全访问控制

10.2.2 数据库加密
10.2.3 事务机制
10.2.4 数据库的并发控制
10.3 SQL Server数据库管理系统的安全性
10.3.1 安全管理
10.3.2 备份与恢复
10.3.3 锁和并发访问控制
10.3.4 使用视图增强安全性
10.3.5 其他安全策略
第11章 无线网络安全
11.1 无线网络安全概述
11.2 无线局域网安全
11.2.1 无线局域网概述
11.2.2 无线局域网面临的安全挑战
11.2.3 无线局域网的安全技术
11.3 无线Ad Hoc网络安全
11.3.1 无线Ad Hoc网络概述
11.3.2 无线Ad Hoc网络面临的安全挑战
11.3.3 无线Ad Hoc网络的安全技术
11.4 无线Sensor网络安全
11.4.1 无线Sensor网络概述
11.4.2 无线Sensor网络面临的安全挑战
11.4.3 无线Sensor网络的安全技术
11.5 无线Mesh网络安全
11.5.1 无线Mesh网络概述
11.5.2 无线Mesh网络面临的安全挑战
11.5.3 无线Mesh网络的安全技术
11.6 无线异构网络安全
11.6.1 无线异构网络概述
11.6.2 无线异构网络面临的安全挑战
11.6.3 无线异构网络的安全技术
第二篇 实 验 篇
第12章 Windows Server 2003服务器安全配置实验
12.1 服务器的安全配置
12.1.1 C盘权限设置
12.1.2 Windows目录权限设置
12.1.3 网络连接设置
12.1.4 服务端口设置
12.2 加强终端服务的安全性
12.2.1 修改终端服务的端口
12.2.2 隐藏登录的用户名
12.2.3 指定用户登录
12.2.4 启动审核
12.2.5 限制、指定连接终端的地址
12.3 防止ASP木马在服务器上运行
12.3.1 使用FileSystemObject组件
12.3.2 使用WScript.Shell组件

12.3.3 使用Shell.Application组件
12.3.4 调用cmd.exe
12.4 网络服务器安全策略
12.4.1 Windows Server 2003的安装
12.4.2 设置和管理账户
12.4.3 网络服务安全管理
12.5 IIS 服务配置
12.5.1 不使用默认的Web站点
12.5.2 删除IIS默认目录
12.5.3 删除虚拟目录
12.5.4 删除不必要的IIS扩展名映射
12.5.5 更改IIS日志的路径
12.6 IPSec配置
12.6.1 IP筛选器
12.6.2 添加入站筛选器
12.6.3 管理筛选器
12.6.4 筛选器激活
12.6.5 选择新建的阻止筛选器
第13章 Web检测实验
13.1 Nikto
13.1.1 安装Nikto
13.1.2 Nikto扫描
13.2 Paros Proxy
13.2.1 安装Paros Proxy
13.2.2 使用Paros Proxy
13.3 Acunetix Web Vulnerability Scanner
13.3.1 安装Acunetix Web Vulnerability Scanner
13.3.2 漏洞检测
13.4 N-Stealth
13.4.1 安装N-Stealth
13.4.2 N-Stealth的使用
第14章 密码实验
14.1 OpenSSL
14.1.1 安装
14.1.2 OpenSSL的使用
14.2 GnuPG/PGP
14.2.1 安装
14.2.2 PGP的使用
第15章 系统扫描实验
15.1 X-Scan
15.2 Superscan
15.3 SSS
第16章 网络监控与嗅探实验
16.1 熟悉Sniffer的基本功能
16.1.1 安装Sniffer
16.1.2 Dashboard
16.1.3 Host Table

16.1.4 Detail
16.1.5 Bar
16.1.6 Matrix
16.2 抓取FTP密码
16.3 抓取HTTP数据包
16.4 抓取Telnet数据包
第17章 破译与攻击实验
17.1 SolarWinds
17.1.1 安装SolarWinds
17.1.2 运行SolarWinds
17.2 Metasploit Framework
17.2.1 安装Metasploit Framework
17.2.2 运行Metasploit Framework
第18章 防火墙实验
18.1 Iptables
18.1.1 初始化工作
18.1.2 开始设置规则
18.1.3 添加规则
18.2 UFW
第19章 入侵检测实验
19.1 Windows下Snort配置
19.1.1 Apache
19.1.2 PHP
19.1.3 Snort
19.1.4 MySQL
19.1.5 Adodb
19.1.6 ACID
19.1.7 Jpgraph
19.1.8 WinPcap
19.1.9 配置Snort
19.1.10 Windows下Snort的使用
19.1.11 Snort命令
19.2 ubuntu下Snort配置
19.2.1 Snort的安装
19.2.2 Snort的使用
19.2.3 入侵检测
参考文献

## 章节摘录

版权页： 插图： 教学提示：随着网络技术的日益更新，计算机网络已从单一化的发展逐渐形成复杂的网络系统。
网络资源的共享为用户带来方便的同时，也使网络产生内部攻击、外部攻击和误操作的安全问题，入侵检测正是作为一种积极主动的安全防护技术应用于网络。
作为网络安全的主要技术之一，入侵检测技术通过对计算机网络中信息的收集与分析，采取相应的安全策略，使网络的安全的风险能有效地降低。
教学目标：掌握入侵检测系统的基本概念与定义，了解入侵检测发展的历程与分类方法，理解入侵检测系统的体系结构与检测技术，并通过对入侵检测系统实例Snort的分析，对入侵检测系统有了一个比较全面的理解。
8.1 入侵检测概述 8.1.1 入侵检测的必要性 传统的网络安全技术主要包括：加密和数字签名机制、身份认证与访问控制机制、认证授权、安全审计、系统脆弱性检测、构筑防火墙系统等。
这些技术都发展得比较成熟，特别是防火墙技术，它能有效地控制内部网络与外部网络之间的访问及数据传送，从而达到保护内部网络的信息不受外部非授权用户的访问和过滤信息的目的，防火墙配置的多样性和防护的有效性使它成为网络安全防线的中流砥柱。
然而任何一种单一的安全技术都并非万能，而且随着攻击者经验日趋丰富，攻击工具与手法的日趋复杂多样，传统单一的安全技术和策略已经无法满足对安全高度敏感的部门的需要。
因此，网络安全的防卫必须采用一种纵深的、多样的手段，形成一个多层次的防护体系，不再是单一的安全技术和安全策略，而是多种技术的融合，关键是各种安全技术能够起到相互补充的作用，这样，即使当某一种措施失去效能时，其他的安全措施也能予以弥补。
传统的安全技术虽然取得了很大的成效，但是它也存在一些固有的缺陷，比如访问控制可以拒绝未授权用户的访问，却并不能防止已授权访问用户获取系统中未授权信息；防火墙可以将危险挡在外面，却无法挡住内部的入侵。
从网络安全的角度看，公司的内部系统被入侵、破坏与泄密是一个严重的问题，以及由此引出的更多有关网络安全的问题都应该引起重视。
据统计，全球80%以上的入侵来自于内部。
因此，传统的安全技术更多的是一种基于被动的防护，而如今的攻击和入侵要求主动地检测、发现和排除安全隐患，正是在这样的环境下，入侵检测系统开始崭露头角，成为安全市场上和研究上新的热点，不仅愈来愈多地受到人们的关注，而且已经开始在各种不同的环境中发挥越来越重要的作用。

## 编辑推荐

《高等学校计算机规划教材:网络安全原理与应用》可作为大专院校网络安全、信息安全及计算机、电子、通信等领域相关专业的教学用书，也可供相关领域从业人员及科研人员参考。
《高等学校计算机规划教材:网络安全原理与应用》实现了理论与实践相结合，是获得网络安全知识的重要途径。

第一图书网, tushu007.com



## 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