

## <<计算机网络安全技术>>

### 图书基本信息

书名：<<计算机网络安全技术>>

13位ISBN编号：9787115283726

10位ISBN编号：7115283729

出版时间：2012-8

出版时间：人民邮电出版社

作者：石淑华 池瑞楠

页数：308

字数：506000

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>

## <<计算机网络安全技术>>

### 内容概要

本书根据高职院校的教学特点和培养目标，全面介绍计算机网络安全的基本框架、基本理论，以及计算机网络安全方面的管理、配置和维护。

全书共8章，主要内容包括计算机网络安全概述、黑客常用的系统攻击方法、计算机病毒、数据加密技术、防火墙技术、Windows

Server的安全、Web的安全性以及网络安全工程。

本书注重实用，以实验为依托，将实验内容融合在课程内容中，使理论紧密联系实际。

本书可作为高职高专计算机及相关专业的教材，也可作为相关技术人员的参考书或培训教材。

# <<计算机网络安全技术>>

## 书籍目录

### 第1章 计算机网络安全概述

- 1.1 网络安全简介
  - 1.1.1 网络安全的重要性
  - 1.1.2 网络脆弱性的原因
  - 1.1.3 网络安全的定义
  - 1.1.4 网络安全的基本要素
  - 1.1.5 典型的网络安全事件
- 1.2 信息安全的发展历程
  - 1.2.1 通信保密阶段
  - 1.2.2 计算机安全阶段
  - 1.2.3 信息技术安全阶段
  - 1.2.4 信息保障阶段
- 1.3 网络安全所涉及的内容
  - 1.3.1 物理安全
  - 1.3.2 网络安全
  - 1.3.3 系统安全
  - 1.3.4 应用安全
  - 1.3.5 管理安全
- 1.4 网络安全防护体系
  - 1.4.1 网络安全的威胁
  - 1.4.2 网络安全的防护体系
  - 1.4.3 数据保密
  - 1.4.4 访问控制技术
  - 1.4.5 网络监控
  - 1.4.6 病毒防护

### 练习题

### 第2章 黑客常用的系统攻击方法

- 2.1 黑客概述
  - 2.1.1 黑客的由来
  - 2.1.2 黑客攻击的动机
  - 2.1.3 黑客入侵攻击的一般过程
- 2.2 目标系统的探测方法
  - 2.2.1 常用的网络探测方法
  - 2.2.2 扫描器概述
  - 2.2.3 端口扫描器演示实验
  - 2.2.4 综合扫描器演示实验
  - 2.2.5 CGI扫描器
  - 2.2.6 专项扫描器
- 2.3 口令破解
  - 2.3.1 口令破解概述
  - 2.3.2 口令破解演示实验
- 2.4 网络监听
  - 2.4.1 网络监听概述
  - 2.4.2 Sniffer演示实验
- 2.5 ARP欺骗攻击

## &lt;&lt;计算机网络安全技术&gt;&gt;

- 2.5.1 ARP欺骗的工作原理
- 2.5.2 交换环境下的ARP欺骗攻击及其嗅探演示实验
- 2.6 木马
  - 2.6.1 木马的工作原理
  - 2.6.2 木马的分类
  - 2.6.3 木马的工作过程
  - 2.6.4 传统木马演示实验
  - 2.6.5 反弹端口木马演示实验
  - 2.6.6 木马的隐藏与伪装方式
  - 2.6.7 木马的启动方式
  - 2.6.8 木马的检测
  - 2.6.9 木马的防御与清除
- 2.7 拒绝服务攻击
  - 2.7.1 拒绝服务攻击概述
  - 2.7.2 拒绝服务攻击原理
  - 2.7.3 拒绝服务攻击演示实验
  - 2.7.4 分布式拒绝服务攻击原理
  - 2.7.5 分布式拒绝服务攻击演示实验
  - 2.7.6 冰盾防火墙的演示实验
- 2.8 缓冲区溢出
  - 2.8.1 缓冲区溢出攻击概述
  - 2.8.2 缓冲区溢出原理
  - 2.8.3 缓冲区溢出演示实验
  - 2.8.4 缓冲区溢出的预防
- 练习题
- 第3章 计算机病毒
  - 3.1 计算机病毒概述
    - 3.1.1 计算机病毒的基本概念
    - 3.1.2 计算机病毒发展简史
    - 3.1.3 计算机病毒的发展历程
  - 3.2 计算机病毒的特征
    - 3.2.1 传染性
    - 3.2.2 破坏性
    - 3.2.3 潜伏性及可触发性
    - 3.2.4 非授权性
    - 3.2.5 隐蔽性
    - 3.2.6 不可预见性
  - 3.3 计算机病毒的分类
    - 3.3.1 按照计算机病毒依附的操作系统分类
    - 3.3.2 按照计算机病毒的传播媒介分类
    - 3.3.3 按照计算机病毒的宿主分类
    - 3.3.4 蠕虫病毒
  - 3.4 计算机病毒的原理与实例
    - 3.4.1 计算机病毒的结构
    - 3.4.2 文件型病毒的实例——CIH病毒
    - 3.4.3 宏病毒
    - 3.4.4 蠕虫病毒的实例——“熊猫烧香”病毒

## <<计算机网络安全技术>>

3.4.5 2008年新病毒的实例——“磁碟机”病毒

3.5 计算机病毒的防治

3.5.1 计算机病毒引起的异常现象

3.5.2 计算机防病毒技术

3.6 防病毒应具有的基础知识

3.6.1 常用的单机杀毒软件

3.6.2 网络防病毒方案

3.6.3 Symantec校园网防病毒案例

3.6.4 选择防病毒软件的标准

练习题

第4章 数据加密技术

4.1 概述

4.1.1 密码学的有关概念

4.1.2 密码学发展的3个阶段

4.1.3 密码学与信息安全的关系

4.2 古典加密技术

4.2.1 替换密码技术

4.2.2 换位密码技术

4.3 对称加密算法及其应用

4.3.1 DES算法及其基本思想

4.3.2 DES算法的安全性分析

4.3.3 其他常用的对称加密算法

4.3.4 对称加密算法在网络安全中的应用

4.4 公开密钥算法及其应用

4.4.1 RSA算法及其基本思想

4.4.2 RSA算法的安全性分析

4.4.3 其他常用的公开密钥算法

4.4.4 公开密钥算法在网络安全中的应用

4.5 数据加密技术的应用

4.5.1 报文鉴别

4.5.2 PGP加密系统演示实验

4.5.3 SSL协议和SET协议

4.5.4 PKI技术及其应用

练习题

第5章 防火墙技术

5.1 防火墙概述

5.1.1 防火墙的基础知识

5.1.2 防火墙的功能

5.1.3 防火墙的局限性

5.2 防火墙分类

5.2.1 软件防火墙和硬件防火墙

5.2.2 单机防火墙和网络防火墙

5.2.3 防火墙的体系结构

5.2.4 防火墙技术分类

5.2.5 防火墙CPU架构分类

5.3 防火墙实现技术原理

5.3.1 包过滤防火墙

## <<计算机网络安全技术>>

- 5.3.2 代理防火墙
- 5.3.3 状态检测防火墙
- 5.3.4 复合型防火墙
- 5.4 防火墙的应用
  - 5.4.1 瑞星个人防火墙的应用
  - 5.4.2 代理服务器的应用
- 5.5 防火墙产品
  - 5.5.1 防火墙的主要参数
  - 5.5.2 选购防火墙的注意点
- 练习题
- 第6章 Windows Server的安全
  - 6.1 Windows Server 2008概述
    - 6.1.1 Windows Server 2008的新特性
    - 6.1.2 Windows Server的模型
  - 6.2 Windows Server 2003的安全模型
    - 6.2.1 Windows Server 2003的安全元素
    - 6.2.2 Windows Server 2003的登录过程
    - 6.2.3 Windows Server 2003的安全认证子系统
    - 6.2.4 Windows Server的安全标识符
  - 6.3 Windows Server的账户管理
    - 6.3.1 Windows Server的安全账号管理器
    - 6.3.2 SYSKEY双重加密账户保护
    - 6.3.3 使用L0phtCrack5审计Windows Server 2003本地账户实验
    - 6.3.4 使用Cain审计Windows Server 2008本地账户实验
    - 6.3.5 账户安全防护
    - 6.3.6 账户安全策略
  - 6.4 Windows Server注册表
    - 6.4.1 注册表的由来
    - 6.4.2 注册表的基本知识
    - 6.4.3 根键
    - 6.4.4 注册表的备份与恢复
    - 6.4.5 注册表的操作
    - 6.4.6 注册表的应用
    - 6.4.7 注册表的权限
    - 6.4.8 注册表的维护工具
  - 6.5 Windows Server常用的系统进程和服务
    - 6.5.1 进程
    - 6.5.2 Windows Server 2003常用的系统进程
    - 6.5.3 进程管理实验
    - 6.5.4 Windows Server的系统服务
    - 6.5.5 Windows Server的系统日志
  - 6.6 Windows Server系统的安全模板
    - 6.6.1 安全模板概述
    - 6.6.2 安全模板的使用
    - 6.6.3 安全配置和分析
- 练习题
- 第7章 Web的安全性

## <<计算机网络安全技术>>

- 7.1 Web的安全性概述
  - 7.1.1 Internet的脆弱性
  - 7.1.2 Web的安全问题
  - 7.1.3 Web安全的实现方法
- 7.2 Web服务器的安全性
  - 7.2.1 Web服务器的作用
  - 7.2.2 Web服务器存在的漏洞
  - 7.2.3 IIS的安全
  - 7.2.4 SSL安全演示实验
- 7.3 脚本语言的安全性
  - 7.3.1 CGI程序的安全性
  - 7.3.2 CGI程序的常见漏洞实例
  - 7.3.3 ASP的安全性
  - 7.3.4 ASP/SQL注入演示实验
- 7.4 Web浏览器的安全性
  - 7.4.1 浏览器本身的漏洞
  - 7.4.2 ActiveX的安全性
  - 7.4.3 Cookie的安全性

### 练习题

## 第8章 网络安全工程

- 8.1 网络安全策略
  - 8.1.1 网络安全策略的制定原则
  - 8.1.2 常用的网络安全策略
- 8.2 网络安全标准
  - 8.2.1 国际上的网络安全标准
  - 8.2.2 国内的网络安全标准
- 8.3 网络安全系统的设计、管理和评估
  - 8.3.1 网络安全系统的设计原则
  - 8.3.2 网络安全系统的管理
  - 8.3.3 网络安全系统的风险评估
- 8.4 典型网络安全工程实例
  - 8.4.1 数据局163/169网络的设计和实施
  - 8.4.2 TF公司信息安全管理体的实施

### 练习题

## 章节摘录

版权页：插图：1.ASP Scanner ASP是基于Server端的脚本运行环境，简单易用，不需要编译和连接，脚本可以在Server端直接运行，并且支持多用户、多线程，在Web开发中得到了广泛的应用。

因为ASP脚本是纯文本格式，所以恶意者通过源代码可以很容易地看到原本不该看到的页面内容。

例如，ASP源代码中通常有系统数据库的连接用户名和口令，恶意者利用此用户名和口令可以轻松地查看数据库中的所有信息（包括系统机密信息），还可能篡改库中信息，造成系统严重损坏，甚至通过这个漏洞来修改管理员的密码等。

因此，保护ASP脚本的源代码非常重要。

保护ASP脚本源代码通常可采用3种方式：第一种是对访问用户进行限制，禁止非法用户访问；第二种是对Server端环境进行处理，提高系统的健壮性；第三种是对源代码进行加工，隐藏或部分隐藏脚本源代码。

这3种方式互为补充，有效设置可以提高脚本源代码的安全性。

ASP Scanner存在的目的在于发现目标系统中是否存在ASP源代码暴露的情况。

2.从各个主要端口取得服务信息的Scanner可以通过这种扫描工具得到某些端口的服务信息，根据此信息，能得知该端口运行的服务是属于哪家公司的产品、什么版本，甚至能根据这些信息判断出操作系统的类型等。

例如，Get\_FTPServer\_Version可以获得对方21端口所运行的FTP服务的版本信息，而Web\_Server\_Version可以获得对方80端口所运行的Web服务的版本信息，这些信息本身虽然没有太大的危害性，但是攻击者可能会根据开放这些端口的服务程序的特定版本来进行特定的攻击。

3.获取操作系统敏感信息的Scanner这类扫描器功能比较强大，可以获取操作系统的各种敏感信息，这些敏感的信息都比较重要，如果被攻击者得到，将直接威胁到系统的安全。

4.数据库Scanner这种扫描工具专门扫描数据库的各种漏洞，国际知名公司ISS还专门有一套Database Scanner，不过该Scanner要正常运行需要提供被扫描数据库的用户名和密码等。

对于一般的数据库Scanner，不需要提供数据库的用户名和密码，当然能扫描的东西也比较有限，一般仅限于猜测数据库的账号和密码等。

除了以上介绍的扫描器外，还有很多不同类型的扫描器，如专门扫描FTP服务器的扫描器、专门对SMTP服务器进行扫描的扫描器，以及用来扫描网关、路由器的扫描器等。



<<计算机网络安全技术>>

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>