

<<网络安全技术>>

图书基本信息

书名：<<网络安全技术>>

13位ISBN编号：9787302293910

10位ISBN编号：7302293910

出版时间：2013-1

出版时间：清华大学出版社

作者：曾湘黔 编

页数：341

字数：549000

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>

## <<网络安全技术>>

### 内容概要

《网络安全技术》全面系统地介绍了计算机网络安全技术。全书共分13章，内容包括网络安全概述、密码学与信息安全、网络安全协议、网络设备常见安全技术、internet安全技术、网络操作系统安全分析及防护、防火墙技术、入侵检测技术、网络嗅探技术、端口扫描技术与漏洞扫描技术、网络病毒防范技术、黑客攻击与防护技术、网络安全解决方案。

《网络安全技术》每章都有思考题，有针对性地帮助读者理解本书的内容。

《网络安全技术》可作为高校计算机及其相关专业“网络安全技术课程”教材，也可供相关的技术人员使用。

书籍目录

第1章 网络安全概述

1.1 网络安全的概念与特征

1.1.1 网络安全的概念

1.1.2 网络安全的特征

1.2 网络面临的安全威胁

1.2.1 网络安全现状

1.2.2 安全威胁分析

1.3 网络安全体系结构

1.3.1 网络安全模型

1.3.2 osi安全体系结构

1.3.3 p2dr模型

1.4 网络安全管理

1.4.1 网络安全管理的法律法规

1.4.2 网络安全评价标准

思考题

第2章 密码学与信息安全

2.1 密码学基础

2.1.1 基本概念

2.1.2 对称密码与非对称密码体制

2.1.3 密码分析的攻击类型

2.1.4 经典密码学

2.2 对称密码体制

2.2.1 基本概念

2.2.2 数据加密标准

2.2.3 加密算法

2.2.4 密钥交换技术

2.3 非对称（公钥）密码

2.3.1 基本思想

2.3.2 rsa公钥密码体制

2.3.3 对称与非对称密钥加密

2.4 认证理论与技术

2.4.1 单向hash函数

2.4.2 md5算法

2.5 身份认证技术

2.6 数字取证技术

2.7 密码学综合应用实例

2.7.1 数字签名技术

2.7.2 数字信封技术

2.7.3 密钥管理技术

2.7.4 消息完整性检验技术

思考题

第3章 网络安全协议

3.1 ssl协议

3.1.1 ssl概述

3.1.2 ssl体系结构与协议

## &lt;&lt;网络安全技术&gt;&gt;

- 3.1.3 ssl安全性分析
- 3.1.4 ssl协议的应用
- 3.2 tls协议
  - 3.2.1 tls概述
  - 3.2.2 tls协议结构
  - 3.2.3 tls记录协议
  - 3.2.4 tls握手协议
  - 3.2.5 tls安全性分析
- 3.3 ssh协议
  - 3.3.1 ssh概述
  - 3.3.2 ssh协议体系结构
  - 3.3.3 ssh传输协议
  - 3.3.4 ssh身份认证协议
  - 3.3.5 ssh连接协议
  - 3.3.6 ssh协议的应用
  - 3.3.7 ssh安全性分析
- 3.4 set协议
  - 3.4.1 set协议概述
  - 3.4.2 set协议基本流程
  - 3.4.3 ssl和set协议比较
  - 3.4.4 set协议安全性分析
- 3.5 ipsec协议
  - 3.5.1 ipsec体系结构
  - 3.5.2 验证文件头协议ah
  - 3.5.3 ipsec安全协议esp
  - 3.5.4 internet安全关联密钥管理协议
- 3.6 qos协议
  - 3.6.1 qos的体系结构
  - 3.6.2 qos的实现机制
- 思考题
- 第4章 网络设备常见安全技术
  - 4.1 局域网络安全技术
    - 4.1.1 网络分段
    - 4.1.2 以交换式集线器代替共享式集线器
    - 4.1.3 vlan的划分
  - 4.2 广域网络安全技术
    - 4.2.1 加密技术
    - 4.2.2 vpn技术
    - 4.2.3 身份认证技术
  - 4.3 vpn技术
    - 4.3.1 隧道技术
    - 4.3.2 加密技术
    - 4.3.3 访问控制技术
  - 4.4 无线网络安全技术
    - 4.4.1 隐藏ssid
    - 4.4.2 mac地址过滤
    - 4.4.3 wep加密
    - 4.4.4 wpa

## <<网络安全技术>>

4.4.5 wpa

4.4.6 ieee 802.11i

4.4.7 ap隔离

4.4.8 ieee 802.1x协议

思考题

第5章 internet安全技术

5.1 internet存在的安全漏洞

5.1.1 internet网络安全概述

5.1.2 网络操作系统安全漏洞

5.1.3 internet应用安全漏洞

5.2 tcp/ip安全性分析

5.2.1 tcp协议工作过程及安全问题

5.2.2 ip协议安全问题

5.2.3 icmp协议的安全问题

5.3 web安全与http访问安全技术

5.3.1 web服务器上的漏洞

5.3.2 如何在web上提高系统安全性和稳定性

5.3.3 http访问安全

5.4 电子邮件安全技术

5.4.1 电子邮件面临的安全问题

5.4.2 电子邮件的安全措施

5.5 telnet安全技术

5.5.1 telnet安全性分析

5.5.2 保障telnet安全的策略分析

5.5.3 安全的telnet系统介绍

5.6 ftp安全技术

5.6.1 ftp工作原理与工作方式

5.6.2 ftp服务器软件漏洞

5.6.3 安全策略

5.7 dns欺骗与防范技术

5.7.1 dns欺骗原理

5.7.2 防范dns欺骗攻击方法

5.8 ip地址欺骗与防范技术

5.8.1 ip地址欺骗原理

5.8.2 ip欺骗的防范措施

5.9 ip地址盗用与防范技术

5.9.1 ip地址盗用的常用方法

5.9.2 ip地址盗用防范技术

5.10 缓冲区溢出攻击与防范技术

5.10.1 缓冲区溢出漏洞的产生原因

5.10.2 缓冲区溢出漏洞的危害性

5.10.3 防范及检测方法

5.11 拒绝服务攻击与防范技术

5.11.1 拒绝服务攻击基本概念

5.11.2 攻击原理

5.11.3 抵御攻击的技术手段

思考题

## <<网络安全技术>>

### 第6章 网络操作系统安全分析及防护

#### 6.1 网络操作系统安全概述

##### 6.1.1 网络操作系统安全问题

##### 6.1.2 网络操作系统安全控制

#### 6.2 windows 2003/xp操作系统安全分析与防护

##### 6.2.1 windows 2003/xp安全机制

##### 6.2.2 windows 2003/xp漏洞分析

##### 6.2.3 windows 2003/xp安全策略

##### 6.2.4 windows 2003/xp安全防护

#### 6.3 unix安全性及防护

##### 6.3.1 unix系统简介

##### 6.3.2 unix系统的安全机制

##### 6.3.3 unix安全漏洞

##### 6.3.4 unix安全策略

##### 6.3.5 unix安全防护

#### 6.4 操作系统安全应用实例

##### 6.4.1 windows系统漏洞的检测与修补

##### 6.4.2 windows中web、ftp服务器的安全配置

##### 6.4.3 unix系统漏洞的检测与修补

##### 6.4.4 unix中web、ftp服务器的安全配置

#### 思考题

### 第7章 防火墙技术

#### 7.1 防火墙基础

##### 7.1.1 防火墙的定义

##### 7.1.2 防火墙的特点

#### 7.2 防火墙的功能与分类

##### 7.2.1 防火墙的功能

##### 7.2.2 防火墙的分类

#### 7.3 防火墙的主要技术

##### 7.3.1 包过滤技术

##### 7.3.2 应用级网关防火墙

##### 7.3.3 深度包过滤技术

#### 7.4 防火墙体系结构

#### 7.5 防火墙配置

##### 7.5.1 网络防火墙配置

##### 7.5.2 防火墙的组网结构

##### 7.5.3 个人防火墙配置

#### 7.6 防火墙的选型

##### 7.6.1 防火墙的选择原则

##### 7.6.2 选择防火墙的两个要素

#### 7.7 主流防火墙产品简介

##### 7.7.1 天融信防火墙

##### 7.7.2 联想防火墙

##### 7.7.3 瑞星防火墙

##### 7.7.4 360 arp防火墙

#### 7.8 防火墙发展动态与趋势

#### 7.9 防火墙部署实例

## <<网络安全技术>>

7.9.1 某校园网防火墙部署

7.9.2 某公司网络防火墙部署

7.9.3 某餐饮企业防火墙方案

思考题

第8章 入侵检测技术

8.1 入侵检测概述

8.1.1 入侵检测原理

8.1.2 入侵检测系统结构

8.1.3 入侵检测系统分类

8.2 入侵检测技术

8.2.1 入侵检测分析模型

8.2.2 误用检测

8.2.3 异常检测

8.2.4 其他检测技术

8.3 入侵检测系统的标准

8.3.1 ietf/idwg

8.3.2 cidf

8.4 入侵检测系统部署

8.4.1 入侵检测系统部署的原则

8.4.2 入侵检测系统部署实例

8.4.3 入侵检测特征库的建立与应用

8.5 典型入侵检测产品简介

8.5.1 入侵检测工具snort

8.5.2 cisco公司的netranger

8.5.3 network associates公司的cybercop

8.5.4 internet security system公司的realsecure

8.5.5 中科网威的“天眼”入侵检测系统

8.6 案例--snort的安装与使用

思考题

第9章 网络嗅探技术

9.1 网络嗅探监听的原理

9.1.1 网卡工作原理

9.1.2 网络嗅探监听的原理

9.1.3 网络嗅探器接入方案

9.1.4 无线局域网嗅探技术原理

9.2 网络监听的防范措施

9.2.1 局域网网络监听的防范措施

9.2.2 无线局域网网络监听的防范措施

9.3 典型嗅探监听工具

9.3.1 tcpdump/windump

9.3.2 sniffit

9.3.3 ettercap

9.3.4 snarp

思考题

第10章 端口扫描技术与漏洞扫描技术

10.1 端口扫描技术

10.1.1 tcp connect()扫描

## &lt;&lt;网络安全技术&gt;&gt;

- 10.1.2 半连接扫描
- 10.1.3 tcp fin扫描
- 10.2 漏洞扫描技术
  - 10.2.1 漏洞扫描概述
  - 10.2.2 漏洞扫描技术的原理
  - 10.2.3 漏洞扫描技术的分类和实现方法
- 10.3 典型的端口扫描与漏洞扫描产品简介
  - 10.3.1 nmap端口扫描工具
  - 10.3.2 scanport端口扫描工具
  - 10.3.3 安铁诺防病毒软件漏洞扫描工具
  - 10.3.4 newt security scanner v1.0网络漏洞扫描工具

## 思考题

## 第11章 网络病毒防范技术

- 11.1 网络病毒基础
  - 11.1.1 计算机病毒的概念
  - 11.1.2 计算机病毒的特征
  - 11.1.3 计算机病毒的结构
  - 11.1.4 网络病毒的特征与传播方式
- 11.2 病毒检测与防范技术
  - 11.2.1 病毒检测技术
  - 11.2.2 病毒防范技术
- 11.3 典型病毒检测与防范产品简介
- 11.4 网络病毒防范实例
  - 11.4.1 病毒特征码的提取及应用技术
  - 11.4.2 宏病毒及防范
  - 11.4.3 网络病毒及防范
  - 11.4.4 恶意代码及防范

## 思考题

## 第12章 黑客攻击与防范技术

- 12.1 黑客基本概念
  - 12.1.1 什么是黑客
  - 12.1.2 黑客发展历史
- 12.2 黑客攻击及防范技术
  - 12.2.1 网络欺骗及防范
  - 12.2.2 嗅探技术及防范
  - 12.2.3 扫描技术及防范
  - 12.2.4 口令破解技术及防范
  - 12.2.5 拒绝服务攻击及防范
  - 12.2.6 缓冲区溢出攻击及防范
  - 12.2.7 木马技术及防范
- 12.3 应用实例
  - 12.3.1 个人计算机防黑技术
  - 12.3.2 配置iis蜜罐抵御黑客攻击

## 思考题

## 第13章 网络安全解决方案

- 13.1 基本概念
  - 13.1.1 网络安全解决方案的层次划分

## <<网络安全技术>>

13.1.2 网络安全解决方案的框架

13.2 网络安全解决方案设计

13.2.1 网络系统状况分析

13.2.2 网络安全需求分析

13.2.3 网络安全解决方案

13.3 网络安全解决方案实例

13.3.1 某银行系统网络安全方案

13.3.2 某市政府中心网络安全方案设计

13.3.3 某电力公司网络安全解决方案

思考题

附录a 英文缩略词汇

参考文献

## 章节摘录

版权页：插图：实际上，这种服务并不能消除服务的抵赖性，也就是说，它并不能防止一方否认另一方对某件已发生的事情所做出的声明。

它能够做的只是提供无可辩驳的证据，以支持快速解决任何这样的纠纷。

抗抵赖服务的出发点不仅仅由于在通信各方之间存在着相互欺骗的可能性，另外它也反映了这样一个现实，即没有任何一个系统是完备的，而且也可能出现通信双方最终达不成一致协议这样的情况。

(1) 数据源的抗抵赖 向数据接收者提供数据来源的证据，以防止发送者否认发送该数据或其内容的任何企图。

(2) 传递过程的抗抵赖 向数据发送者提供数据已到目的地的证据，以防止收信者否认接收该数据或其内容后的任何事后的企图。

2.安全机制 为了支持以上的安全服务，ISO安全体系结构定义了8大类安全机制：加密机制、数字签名机制、访问控制机制、数据完整性机制、鉴别交换机制、通信业务填充机制、路由控制机制和公证机制。

这些安全机制可以设置在适当的层次上，以便提供某些安全服务。

1) 加密机制 加密是提供数据保护最常用的方法。

加密算法按密钥的类型可分为对称密钥算法和非对称密钥（也称公开密钥）算法；按密码体制可分为序列密码算法和分组密码算法。

这些算法具有不同的优缺点，根据加密的层次和加密对象可采用不同的算法。

由于加密机制的存在，就有密钥管理机制。

2) 数字签名机制 在通信双方交换数据时，为防止否认、伪造、篡改、冒充等，采用数字签名技术。

数字签名机制还规定了两个过程：一是对数据单元签名，二是验证已签名的数据单元。

签名机制的本质特征是只能使用签名者私有信息签名。

因此，当验证签名时，可在事后的任何时候向第三方（如审查员或仲裁员）证实只有私有信息的唯一持有者才能产生这个签名。

3) 访问控制机制 访问控制机制是按照事先确定的规划，决定主题对客体的访问是否合法。

当主体试图非法使用未经授权使用的资源（客体）时，访问机制的功能将拒绝这一企图，并可附带报告这一事件给审计跟踪系统，审计跟踪产生一个报警或形成部分追踪审计。

访问控制机制的实现常常基于一种或多种机制措施，如访问控制信息库、鉴别信息（如口令）、权力、安全标志、试图访问的时间、试图访问的路由和访问的持续时间等。

4) 数据完整性机制 数据完整性包括两种形式：数据单元完整性和数据单元序列的完整性。

保证数据完整性的一般方法是：发送实体在数据单元上加标记，这个标记是数据本身的函数，是经过加密的；接收实体产生对应的标记，并将所产生的标记与接收到标记相比较，以确定在传输过程中疏忽是否被修改过。

数据单元序列的完整性是要求数据编号的连续性和时间标记的正确性（不是过时的），以防止假冒、丢失、重发、插入或修改数据。

5) 鉴别交换机制 鉴别交换机制是以交换信息的方式来确认实体身份的机制。

用于鉴别交换的技术有：口令。

由发方实体提供，收方实体检测。

密码技术。

将交换的数据加密，只有合法用户才能解密。

使用该实体的特征或拥有物。

这时采用的技术是指纹识别和身份卡等。

编辑推荐

《普通高等学校网络工程专业规划教材:网络安全技术》每章都有思考题,有针对性地帮助读者理解《普通高等学校网络工程专业规划教材:网络安全技术》的内容。

《普通高等学校网络工程专业规划教材:网络安全技术》可作为高校计算机及其相关专业“网络安全技术课程”教材,也可供相关的技术人员使用。

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>