

<<信息安全技术教程>>

图书基本信息

书名：<<信息安全技术教程>>

13位ISBN编号：9787302305248

10位ISBN编号：7302305242

出版时间：2013-1

出版时间：清华大学出版社

作者：杜彦辉

页数：383

字数：615000

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>

## <<信息安全技术教程>>

### 内容概要

《信息安全技术教程》从信息安全领域的基础入手，系统、全面地介绍信息安全理论和实践知识，并尽可能地涵盖信息安全技术的主要内容，对发展起来的新技术做详细介绍。此外，还增加实践内容，介绍相关工具软件以及具体信息安全技术实施的具体方法。

《信息安全技术教程》共19章，主要内容包括信息安全基础知识、密码技术、认证技术、安全协议、安全事件处理、访问控制与权限设置、防火墙技术、入侵检测、系统安全扫描技术、病毒防范与过滤技术、信息安全风险评估技术、灾准备份与恢复技术、计算机与网络取证技术、操作系统安全、操作系统加固、安全审计原则与实践、应用开发安全技术、信息安全建设标准、构建企业安全实践等。

《信息安全技术教程》结构清晰、内容翔实，具有很强的可读性，适合作为高等院校信息安全专业本科生和相关专业的高年级本科生或研究生教材，也适合供相关科研人员和对信息安全相关技术感兴趣的读者阅读。

# <<信息安全技术教程>>

## 书籍目录

### 第1章 信息网络安全基本概念

- 1.1 信息安全基础
- 1.2 信息安全面临的挑战
- 1.3 信息安全五性
- 1.4 信息安全风险分析

习题

课后实践与思考

### 第2章 密码技术

- 2.1 密码学基础
  - 2.1.1 密码学历史及密码系统组成
  - 2.1.2 密码的作用
  - 2.1.3 密码算法
- 2.2 对称密码算法
  - 2.2.1 des算法
  - 2.2.2 对称密码算法存在的问题
- 2.3 非对称密码算法
  - 2.3.1 rsa算法
  - 2.3.2 非对称密码算法存在的问题

#### 2.4 数字签名技术

- 2.4.1 数字签名生成
- 2.4.2 数字签名认证

#### 2.5 数字证书

- 2.5.1 数字证书的工作原理
- 2.5.2 数字证书的颁发机制
- 2.5.3 数字证书的分类

#### 2.6 信息隐藏技术

- 2.6.1 信息隐藏
  - 2.6.2 数字水印
  - 2.6.3 数字隐写
- #### 2.7 邮件加密软件pgp
- 2.7.1 pgp加密原理
  - 2.7.2 pgp安装
  - 2.7.3 pgp生成密钥
  - 2.7.4 pgp加解密

习题

课后实践与思考

### 第3章 认证技术

- 3.1 基本概念
- 3.2 认证组成
- 3.3 认证技术
  - 3.3.1 口令认证
  - 3.3.2 公钥认证
  - 3.3.3 远程认证
  - 3.3.4 匿名认证
  - 3.3.5 基于数字签名的认证

## <<信息安全技术教程>>

习题

课后实践

### 第4章 安全协议

4.1 tcp/ip工作原理

4.2 tcp/ip协议安全

4.2.1 s/mime

4.2.2 web安全

4.2.3 set

4.2.4 传输层安全

4.2.5 虚拟专用网络

4.2.6 拨号用户远程认证服务

4.3 kerberos

4.3.1 kerberos的概念

4.3.2 kerberos服务所要满足的目标

4.3.3 kerberos认证过程

4.4 安全套接层ssl

4.4.1 ssl的概念

4.4.2 ssl连接

4.5 因特网协议安全

4.5.1 ipsec协议分析

4.5.2 ipsec加密模式

4.6 点对点协议

4.6.1 ppp的组成

4.6.2 ppp工作流程

4.6.3 ppp认证

习题

课后实践与思考

### 第5章 安全事件处理

5.1 攻击及其相关概念

5.1.1 安全事件

5.1.2 安全事件类型

5.2 安全事件管理方法

5.2.1 安全事件预防

5.2.2 安全事件处理标准的制定

5.2.3 对安全事件的事后总结

5.3 恶意代码

5.3.1 病毒

5.3.2 蠕虫

5.3.3 特洛伊木马

5.3.4 网络控件

5.4 常见的攻击类型

5.4.1 后门攻击

5.4.2 暴力攻击

5.4.3 缓冲区溢出

5.4.4 拒绝服务攻击

5.4.5 中间人攻击

5.4.6 社会工程学

## <<信息安全技术教程>>

5.4.7 对敏感系统的非授权访问

5.5 无线网络安全

5.5.1 无线网络基础

5.5.2 无线网络协议标准

5.5.3 无线网络安全

5.5.4 无线局域网存在的安全问题

5.6 传感网络

5.6.1 传感网络的基本元素

5.6.2 无线传感网络安全

习题

课后实践与思考

### 第6章 访问控制与权限设置

6.1 访问控制基本概念

6.2 访问控制规则的制定原则

6.3 访问控制分类

6.3.1 自主访问控制

6.3.2 强制访问控制

6.3.3 基于角色的访问控制

6.4 访问控制实现技术

6.5 访问控制管理

6.6 访问控制模型

6.6.1 状态机模型

6.6.2 bell-lapadula模型

6.6.3 biba模型

6.6.4 clark-wilson模型

6.7 文件和数据所有权

6.8 相关的攻击方法

习题

课后实践与思考

### 第7章 防火墙技术

7.1 边界安全设备

7.1.1 路由器

7.1.2 代理服务器

7.1.3 防火墙

7.2 防火墙的种类

7.2.1 硬件防火墙和软件防火墙

7.2.2 包过滤防火墙

7.2.3 状态检测防火墙

7.3 防火墙拓扑结构

7.3.1 屏蔽主机

7.3.2 屏蔽子网防火墙

7.3.3 双重防火墙

7.4 防火墙过滤规则库

7.4.1 概述

7.4.2 特殊规则

习题

课后实践与思考

## <<信息安全技术教程>>

### 第8章 入侵检测

8.1 入侵检测的概念与基本术语

8.2 入侵检测系统的检测机制

8.3 入侵检测系统

8.3.1 入侵检测系统的设计准则

8.3.2 基于网络的入侵检测系统 ( nids )

8.3.3 基于主机的入侵检测系统 ( hids )

8.3.4 nids与hids比较

8.3.5 其他类型的入侵检测系统

8.4 入侵检测系统实现

8.5 入侵检测系统产品的选择

8.6 入侵检测的发展趋势

8.7 snort简介

8.7.1 snort的工作原理

8.7.2 snort在windows下的安装与部署

8.7.3 启动snort

习题

课后实践

### 第9章 系统安全扫描技术

9.1 系统安全扫描的技术基础

9.2 操作系统指纹识别工具

9.3 网络和服务扫描工具

9.4 ip栈指纹识别

9.5 telnet查询

9.6 tcp/ip服务漏洞

9.7 tcp/ip简单服务

9.8 安全扫描总结

习题

课后实践与思考

### 第10章 病毒防范与过滤技术

10.1 内容过滤技术

10.1.1 过滤的种类

10.1.2 内容过滤的位置

10.1.3 内容过滤的层次

10.1.4 过滤内容

10.2 病毒过滤

10.2.1 定义

10.2.2 病毒感染方式

10.2.3 病毒感染源

10.2.4 病毒的种类

10.2.5 病毒防范技术

10.3 垃圾邮件防范技术

10.3.1 垃圾邮件的定义及危害

10.3.2 反垃圾邮件技术

10.3.3 反垃圾邮件典型案例

习题

课后实践与思考

## <<信息安全技术教程>>

### 第11章 信息安全风险评估技术

- 11.1 系统安全策略
- 11.2 系统安全要求分析
- 11.3 信息安全风险识别
  - 11.3.1 人为因素
  - 11.3.2 自然灾害
  - 11.3.3 基础架构故障
- 11.4 信息安全威胁分析
- 11.5 信息安全威胁分析方法
- 11.6 系统漏洞识别与评估
  - 11.6.1 硬件系统漏洞
  - 11.6.2 软件系统漏洞
- 11.7 安全监控与审计
- 11.8 安全评估工具使用

#### 习题

#### 课后实践与思考

### 第12章 灾准备份与恢复技术

- 12.1 灾难预防
- 12.2 系统灾难响应
- 12.3 灾难恢复委员会
- 12.4 恢复进程
- 12.5 使系统时刻处于准备之中
- 12.6 灾准备份技术
  - 12.6.1 灾准备份中心
  - 12.6.2 灾准备份与恢复技术
  - 12.6.3 数据备份技术
  - 12.6.4 数据的存储技术
  - 12.6.5 cdp连续数据保护技术

#### 习题

#### 课后实践与思考

### 第13章 计算机与网络取证技术

- 13.1 基本概念
- 13.2 计算机取证技术
  - 13.2.1 计算机取证基本元素
  - 13.2.2 计算机取证过程
  - 13.2.3 计算机证据分析
- 13.3 网络取证
- 13.4 取证工具
  - 13.4.1 计算机取证工具
  - 13.4.2 网络取证工具

#### 习题

#### 课后实践与思考

### 第14章 操作系统安全

- 14.1 操作系统安全基础
  - 14.1.1 操作系统安全术语和概念
  - 14.1.2 系统安全规划
  - 14.1.3 内置安全子系统和机制

## <<信息安全技术教程>>

14.2 操作系统安全原则与实践

14.3 windows系统安全设计

14.4 unix和linux安全设计

14.5 系统备份

14.6 典型的系统安全威胁

14.7 击键记录

14.8 常见windows系统风险

14.9 常见unix系统风险

14.10 操作系统扫描和系统标识

习题

课后实践与思考

### 第15章 操作系统加固

15.1 操作系统加固的原则和做法

15.2 操作系统安全维护

15.3 安装安全检查软件

15.3.1 windows安全检查列表

15.3.2 unix安全检查列表

15.4 文件系统安全

15.5 操作系统用户管理安全

15.5.1 windows账户安全策略

15.5.2 unix账户安全策略

15.6 操作系统日志功能

习题

课后实践与思考

### 第16章 安全审计原则与实践

16.1 设置日志记录

16.1.1 需要记录的行为

16.1.2 记录保留时间

16.1.3 设置报警系统

16.1.4 windows日志记录

16.1.5 unix日志记录

16.2 日志数据分析

16.3 系统日志安全维护

16.4 系统安全审计

16.4.1 审计小组

16.4.2 审计工具

16.4.3 审计结果处理

习题

### 第17章 应用开发安全技术

17.1 数据库安全技术

17.1.1 数据库系统面临的风险

17.1.2 数据库系统安全

17.1.3 数据库系统安全防范技术

17.2 软件开发安全技术

17.2.1 软件安全问题原因

17.2.2 软件安全开发模型

17.2.3 软件安全开发策略



## <<信息安全技术教程>>

### 17.3 电子商务安全策略

#### 17.3.1 电子商务安全基础

#### 17.3.2 电子支付系统安全

#### 17.3.3 生物识别安全技术

### 17.4 web服务安全技术

#### 17.4.1 web服务概述

#### 17.4.2 web服务安全

#### 习题

#### 课后实践与思考

## 第18章 信息安全建设标准

### 18.1 通用安全原则

#### 18.1.1 通用原则

#### 18.1.2 安全策略

#### 18.1.3 安全管理工具

#### 18.1.4 物理安全

#### 18.1.5 人员安全

### 18.2 安全标准

#### 18.2.1 tcsec

#### 18.2.2 itsec

#### 18.2.3 ctcepc

#### 18.2.4 fips

#### 18.2.5 bs7799系列 ( iso/iec 27000系列 )

#### 18.2.6 iso/iec tr 13335系列

#### 18.2.7 sse-cmm

#### 18.2.8 itil和bs15000

#### 18.2.9 cc

#### 18.2.10 cobit

#### 18.2.11 nist sp800系列

### 18.3 安全法规

#### 习题

#### 课后实践

## 第19章 构建企业安全实践

### 19.1 构建企业安全案例

### 19.2 企业业务连续性计划

#### 19.2.1 漏洞评估

#### 19.2.2 实施控制

#### 19.2.3 计划维护

### 19.3 灾难恢复计划

#### 19.3.1 选择维护团队

#### 19.3.2 制订灾难恢复计划

#### 19.3.3 培训和测试

#### 19.3.4 实施计划

#### 19.3.5 计划的维护

### 19.4 数据分类

#### 19.4.1 安全许可

#### 19.4.2 必备知识

#### 19.4.3 分类系统

<<信息安全技术教程>>

习题

课后实践与思考

实例小结

附录a

附表a-1 维护常见安全漏洞列表的网站

附表a-2 安全扫描工具的网站

附表a-3 操作系统指纹识别工具

附表a-4 安全漏洞邮寄列表

附表a-5 黑客大会

参考文献

## 章节摘录

版权页：插图：3.3 认证技术 随着网络安全技术的不断发展，已经出现了多种不同的认证技术。根据不同的功能水平和安全需要，这些认证技术可以单独使用，也可以同时使用。

主要的认证技术包括口令认证、公开密钥认证、远程认证、匿名认证和数字签名认证。

3.3.1 口令认证 口令认证是最古老、最简单的一种认证方法，经常作为系统的默认设置。

口令认证包括可重用口令认证、一次性口令认证、挑战应答口令认证和混合口令认证。

1. 可重用口令认证 可重用口令认证有两种类型：用户（user）认证和客户端（client）认证。

用户认证通常由申请使用系统资源的用户发起。

接到用户的资源使用请求后，服务器向用户索要用户名和口令，然后将这些信息和数据库上的信息进行比对，如果匹配成功，用户请求被允许，可以访问系统资源。

例如，人们在使用电脑时，需要输入用户名和口令，就是最简单的用户认证。

客户端认证 一般情况下，用户请求服务器的认证，然后被授权使用系统资源。

用户通过认证并不意味着可以自由使用任何想要的系统资源。

通过认证只是说明用户被授权使用所请求的那些资源，但并不能超过这个限度。

这种类型的认证就叫做客户端认证。

这种认证根据用户的身份，使用户受限访问系统的资源。

可重用口令认证方法简单、运行速度快、使用广泛，但也存在着一系列的问题。

为了避免记忆复杂口令，用户常会选择简单口令，或把口令值记录下来，增加了安全隐患。

同时，随着计算机计算水平的提高，通过蛮力攻击能够很容易破解系统的口令值。

2. 一次性口令认证 一次性口令认证也被称为会话认证，认证中的口令只能被使用一次，然后被丢弃，从而减少了口令被破解的可能性。

在一次性口令认证中，口令值通常是被加密的，避免明文形式的口令被攻击者截获。

最常见的一次性口令认证方案是S / Key和Token方案。

（1）S / Key口令 这种口令认证基于MD4和MD5加密算法产生，采用客户—服务器模式。

客户端负责用hash函数产生每次登录使用的口令，服务器端负责一次性口令的验证，并支持用户密钥的安全交换。

在认证的预处理过程中，服务器将种子以明文形式发送给客户端，客户端将种子和密钥拼接在一起得到S。

然后，客户端对S进行hash运算得到一系列一次性口令。

也就是说，第一次口令是通过对S进行N次hash运算得到，下一次的口令是通过对S进行N—1次hash运算得到。

在服务器端保存着用户上一次成功登录的口令值，因此，当用户访问系统时，服务器只需要将本次传输过来的口令进行一次hash运算。

如果得到结果和存储的值一致，就验证了用户身份的正确性。

## <<信息安全技术教程>>

### 编辑推荐

《教育部实用型信息技术人才培养系列教材:信息安全技术教程》结构清晰、内容翔实，具有很强的可读性，适合作为高等院校信息安全专业本科生和相关专业的高年级本科生或研究生教材，也适合供相关科研人员和对信息安全相关技术感兴趣的读者阅读。

<<信息安全技术教程>>

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>