

信息安全导论

信息安全导论书籍信息

书名：信息安全导论

I S B N : 9 7 8 7 1 1 5 5 3 2 0 7 7

作者：李冬冬 & n b s p ;

出版社：人民邮电出版社

出版时间：2 0 2 0 - 0 9

页数：

价格：4 6 . 0 0

纸张：胶版纸

装帧：平装 - 胶订

开本：1 6 开

语言：未知

丛书：

T A G : 教材 & n b s p ; 研究生 / 本科 / 专科教材 & n b s p ; 工学 & n b s p ;

豆瓣评分：

版权说明：本站所提供下载的 P D F 图书仅提供预览和简介，请支持正版图书。

信息来源：信息安全导论 t x t e p u b k i n d l e 下载 电子书 2 0 2 4 - 书

信息安全导论

信息安全导论书籍简介

全书介绍了信息安全的基本概念、身份认证技术、授权与访问控制技术、操作系统安全、网络安全协议、网络攻击技术、边界防御技术、入侵检测技术、Web安全、无线安全等内容。每章均配有习题，包括选择题、填空题、论述题和实践题，帮助读者巩固本章所学理论知识，并进行实践尝试。

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。

信息来源：信息安全导论 txt epub kindle 下载 电子书 2024 - 书

信息安全导论

信息安全导论目录

- 1.1 信息化发展及其带来的安全问题 1
 - 1.1.1 信息化发展状况 1
 - 1.1.2 当前信息安全问题 2
- 1.2 信息安全基础 5
 - 1.2.1 什么是信息安全 5
 - 1.2.2 信息安全的发展历程 7
 - 1.2.3 安全威胁 8
 - 1.2.4 安全攻击 9
- 1.3 安全体系结构与模型 10
 - 1.3.1 开放系统互连安全体系结构 10
 - 1.3.2 信息安全模型 14
 - 1.3.3 信息保障技术框架 16
- 1.4 信息安全国际标准 19
 - 1.4.1 可信计算机系统评估准则 20
 - 1.4.2 信息技术安全评估准则 20
 - 1.4.3 通用安全评估准则 21
 - 1.4.4 BS 7799标准 21
 - 1.4.5 ISO/IEC 27000系列标准 21
- 1.5 我国的网络安全等级保护和涉密信息系统分级保护 22
 - 1.5.1 网络安全等级保护 22
 - 1.5.2 涉密信息系统分级保护 24
- 1.6 我国信息安全法律法规 25
 - 1.6.1 信息安全相关法律 25
 - 1.6.2 信息安全相关法规 27

1 . 7 小结 2 8

习题 2 8

第2章 网络攻击与防御技术 3 1

2 . 1 网络攻击概述 3 1

2 . 2 社会工程学攻击 3 2

2 . 2 . 1 什么是社会工程学攻击 3 2

2 . 2 . 2 社会工程学攻击的常见形式 3 3

2 . 2 . 3 如何防御社会工程学攻击 3 4

2 . 3 扫描器 3 5

2 . 3 . 1 什么是扫描器 3 5

2 . 3 . 2 扫描器的分类 3 5

2 . 3 . 3 扫描技术 3 6

2 . 4 嗅探器 3 8

2 . 4 . 1 什么是嗅探器 3 8

2 . 4 . 2 嗅探器的工作原理 3 9

2 . 4 . 3 如何防御嗅探器 4 0

2 . 5 口令攻击和口令安全 4 1

2 . 5 . 1 口令猜测 4 1

2 . 5 . 2 口令破解 4 2

2 . 5 . 3 彩虹表 4 3

2 . 5 . 4 口令安全 4 3

2 . 6 漏洞利用 4 4

2 . 6 . 1 缓冲区溢出漏洞 4 4

2 . 6 . 2 缓冲区溢出的利用 4 5

2 . 6 . 3 缓冲区溢出的保护方法 4 7

2 . 6 . 4 漏洞利用实例 4 8

| | | |
|-------|---------------|----|
| 2.7 | 拒绝服务攻击 | 49 |
| 2.7.1 | 什么是拒绝服务攻击 | 49 |
| 2.7.2 | 拒绝服务攻击的类型 | 49 |
| 2.7.3 | 分布式拒绝服务攻击 | 50 |
| 2.7.4 | 如何防御分布式拒绝服务攻击 | 51 |
| 2.8 | A P T攻击 | 52 |
| 2.8.1 | 什么是A P T攻击 | 52 |
| 2.8.2 | 如何防御A P T攻击 | 53 |
| 2.9 | 小结 | 54 |
| | 习题 | 54 |
| 第3章 | 恶意代码及其防范 | 56 |
| 3.1 | 恶意代码概述 | 56 |
| 3.1.1 | 恶意代码的概念及发展 | 56 |
| 3.1.2 | 恶意代码的分类及命名 | 58 |
| 3.1.3 | 恶意代码的基本特点 | 59 |
| 3.1.4 | 恶意代码的基本作用机制 | 61 |
| 3.1.5 | 恶意代码的基本防范方法 | 61 |
| 3.2 | 蠕虫病毒 | 62 |
| 3.2.1 | 蠕虫病毒概述 | 62 |
| 3.2.2 | 蠕虫病毒的传播机制 | 62 |
| 3.2.3 | 蠕虫病毒的防御 | 64 |
| 3.3 | 木马病毒 | 65 |
| 3.3.1 | 木马病毒概述 | 65 |
| 3.3.2 | 木马病毒的原理 | 66 |
| 3.3.3 | 木马病毒的防御 | 69 |
| 3.4 | 僵尸网络 | 70 |

| | | |
|-------|-----------------|-----|
| 3.4.1 | 僵尸网络的定义 | 70 |
| 3.4.2 | 僵尸网络的功能结构 | 71 |
| 3.4.3 | 僵尸网络的工作机制 | 72 |
| 3.4.4 | 僵尸网络的危害 | 73 |
| 3.4.5 | 僵尸网络的防御方法 | 75 |
| 3.5 | 恶意代码分析技术 | 75 |
| 3.5.1 | 静态分析方法 | 75 |
| 3.5.2 | 动态分析方法 | 77 |
| 3.5.3 | 恶意代码分析实例 | 78 |
| 3.6 | 恶意代码检测方法 | 83 |
| 3.7 | 小结 | 84 |
| | 习题 | 84 |
| 第4章 | 身份认证技术 | 87 |
| 4.1 | 身份认证概述 | 87 |
| 4.1.1 | 身份认证的概念 | 88 |
| 4.1.2 | 身份认证的分类 | 88 |
| 4.1.3 | 身份认证所面临的安全攻击 | 89 |
| 4.2 | 常见的身份认证方式 | 90 |
| 4.2.1 | 基于口令认证 | 90 |
| 4.2.2 | 基于智能卡认证 | 91 |
| 4.2.3 | 基于密码技术的一次性口令认证 | 92 |
| 4.2.4 | 基于生物特征认证 | 93 |
| 4.3 | 身份认证协议 | 97 |
| 4.3.1 | Kerberos 认证协议 | 97 |
| 4.3.2 | X.509 认证协议 | 102 |
| 4.4 | 数字证书与公钥基础设施 PKI | 104 |

| | | |
|--------------------|----------------|-----|
| 4.4.1 | 数字证书 | 104 |
| 4.4.2 | PKI的概念 | 108 |
| 4.4.3 | PKI提供的安全服务 | 109 |
| 4.4.4 | PKI的组成 | 109 |
| 4.5 | 其他认证技术 | 111 |
| 4.5.1 | 单点登录与统一身份认证 | 111 |
| 4.5.2 | 拨号认证协议 | 112 |
| 4.6 | 小结 | 113 |
| 习题 113 | | |
| 第5章 访问控制、授权与审计 116 | | |
| 5.1 | 访问控制 | 116 |
| 5.1.1 | 访问控制概述 | 116 |
| 5.1.2 | 常见的访问控制技术 | 118 |
| 5.2 | 授权与PMI | 129 |
| 5.2.1 | 授权描述 | 129 |
| 5.2.2 | PMI | 129 |
| 5.3 | 安全审计 | 132 |
| 5.3.1 | 安全审计的概念 | 132 |
| 5.3.2 | 安全审计系统的分类 | 133 |
| 5.3.3 | 安全审计的数据来源与实现原理 | 135 |
| 5.4 | 小结 | 136 |
| 习题 137 | | |
| 第6章 操作系统安全 139 | | |
| 6.1 | 操作系统安全概述 | 139 |
| 6.1.1 | 操作系统安全的概念 | 139 |
| 6.1.2 | 操作系统的安全配置 | 143 |

| | | |
|------------------|---------------------|-----|
| 6.1.3 | 操作系统的安全设计 | 144 |
| 6.1.4 | 操作系统安全性的设计原则及方法 | 144 |
| 6.2 | Windows 操作系统的安全特性 | 146 |
| 6.2.1 | Windows 操作系统的安全模型 | 147 |
| 6.2.2 | Windows 操作系统的用户登录过程 | 149 |
| 6.2.3 | Windows 操作系统的资源访问 | 150 |
| 6.2.4 | Windows 操作系统的安全审计 | 153 |
| 6.3 | Linux 操作系统的安全特性 | 154 |
| 6.3.1 | Linux 操作系统的安全机制 | 154 |
| 6.3.2 | 提高Linux操作系统安全的策略 | 157 |
| 6.4 | 小结 | 158 |
| 习题 158 | | |
| 第7章 网络边界防御技术 161 | | |
| 7.1 | 网络边界防御概述 | 161 |
| 7.1.1 | 网络边界 | 161 |
| 7.1.2 | 边界防御技术 | 162 |
| 7.2 | 防火墙技术 | 163 |
| 7.2.1 | 防火墙概述 | 163 |
| 7.2.2 | 防火墙的体系结构 | 168 |
| 7.2.3 | 防火墙的关键技术 | 170 |
| 7.2.4 | 虚拟防火墙 | 177 |
| 7.3 | 虚拟专用网技术 | 177 |
| 7.3.1 | 虚拟专用网概述 | 177 |
| 7.3.2 | 虚拟专用网的分类 | 178 |
| 7.3.3 | 虚拟专用网的关键技术 | 179 |
| 7.4 | 安全网关 | 180 |

| | | |
|-------|-----------------|-----|
| 7.5 | 小结 | 181 |
| | 习题 | 182 |
| 第8章 | 入侵检测技术 | 184 |
| 8.1 | 入侵检测系统概述 | 184 |
| 8.1.1 | 什么是入侵检测系统 | 184 |
| 8.1.2 | 入侵检测系统框架 | 185 |
| 8.1.3 | 入侵检测系统的分类 | 186 |
| 8.1.4 | 入侵检测系统的部署 | 191 |
| 8.2 | 入侵检测技术 | 191 |
| 8.2.1 | 误用检测 | 192 |
| 8.2.2 | 异常检测 | 193 |
| 8.3 | 入侵检测系统实例——Snort | 195 |
| 8.3.1 | Snort简介 | 195 |
| 8.3.2 | Snort的特点 | 195 |
| 8.3.3 | Snort的整体架构 | 196 |
| 8.3.4 | Snort规则 | 197 |
| 8.3.5 | Snort的入侵检测流程 | 201 |
| 8.4 | 入侵防御系统 | 202 |
| 8.4.1 | 什么是入侵防御系统 | 202 |
| 8.4.2 | 入侵防御系统的分类 | 203 |
| 8.4.3 | 入侵防御系统的工作方式 | 204 |
| 8.5 | 小结 | 205 |
| | 习题 | 205 |
| 第9章 | 网络安全协议 | 207 |
| 9.1 | 网络安全协议概述 | 207 |
| 9.1.1 | TCP/IP体系结构概述 | 207 |

| | | |
|--------------|----------------------|-----|
| 9.1.2 | TCP / IP的安全性分析 | 209 |
| 9.1.3 | TCP / IP体系结构中各层的安全协议 | 212 |
| 9.2 | IPSec | 213 |
| 9.2.1 | IPv4和IPv6 | 213 |
| 9.2.2 | IPSec简介 | 215 |
| 9.2.3 | 安全关联与安全策略 | 216 |
| 9.2.4 | AH、ESP和IKE协议 | 218 |
| 9.2.5 | IPSec的工作模式 | 220 |
| 9.3 | TLS / SSL协议 | 221 |
| 9.3.1 | TLS / SSL协议简介 | 221 |
| 9.3.2 | TLS握手协议 | 223 |
| 9.3.3 | TLS修改密文规约协议 | 225 |
| 9.3.4 | TLS告警协议 | 225 |
| 9.3.5 | TLS记录协议 | 225 |
| 9.4 | SSH协议 | 227 |
| 9.4.1 | SSH协议简介 | 227 |
| 9.4.2 | SSH协议的结构 | 227 |
| 9.4.3 | SSH协议的工作过程 | 228 |
| 9.5 | 小结 | 230 |
| 习题 | | 231 |
| 第10章 Web应用安全 | | 233 |
| 10.1 | Web安全概述 | 233 |
| 10.1.1 | Web体系结构 | 233 |
| 10.1.2 | Web安全威胁 | 239 |
| 10.1.3 | Web安全防范 | 240 |
| 10.2 | Web安全 | 242 |

| | | |
|----------------------|--------------------------------|-------|
| 1 0 . 2 . 1 | 浏览器及安全 | 2 4 2 |
| 1 0 . 2 . 2 | 服务器软件及安全 | 2 4 3 |
| 1 0 . 2 . 3 | W e b 框架安全 | 2 4 3 |
| 1 0 . 3 | W e b 安全攻防技术 | 2 4 6 |
| 1 0 . 3 . 1 | X S S 攻击及其防御 | 2 4 6 |
| 1 0 . 3 . 2 | C S R F 攻击及其防御 | 2 4 8 |
| 1 0 . 3 . 3 | C l i c k J a c k i n g 攻击及其防御 | 2 5 1 |
| 1 0 . 3 . 4 | S Q L 注入攻击及其防御 | 2 5 2 |
| 1 0 . 4 | 小结 | 2 5 5 |
| 习题 2 5 5 | | |
| 第 1 1 章 无线网络安全 2 5 8 | | |
| 1 1 . 1 | 无线网络面临的安全威胁 | 2 5 8 |
| 1 1 . 2 | 无线蜂窝网络的安全性 | 2 6 1 |
| 1 1 . 2 . 1 | G S M 的安全性 | 2 6 2 |
| 1 1 . 2 . 2 | C D M A 的安全性 | 2 6 3 |
| 1 1 . 2 . 3 | 3 G 的安全性 | 2 6 4 |
| 1 1 . 2 . 4 | L T E 的安全性 | 2 6 6 |
| 1 1 . 2 . 5 | 5 G 系统的安全性 | 2 6 9 |
| 1 1 . 3 | 无线局域网的安全性 | 2 7 0 |
| 1 1 . 3 . 1 | 8 0 2 . 1 1 b 标准介绍 | 2 7 0 |
| 1 1 . 3 . 2 | 8 0 2 . 1 1 i 标准介绍 | 2 7 3 |
| 1 1 . 3 . 3 | W A P I 标准介绍 | 2 7 6 |
| 1 1 . 4 | 移动 A d h o c 网络的安全性 | 2 7 8 |
| 1 1 . 4 . 1 | 移动 A d h o c 网络简介 | 2 7 8 |
| 1 1 . 4 . 2 | 移动 A d h o c 网络的安全性 | 2 7 9 |
| 1 1 . 4 . 3 | 移动 A d h o c 网络安全的密钥管理和认证技术 | 2 8 0 |

| | | |
|-------------|------------------------|-------|
| 1 1 . 4 . 4 | 移动 A d h o c 网络的安全路由技术 | 2 8 4 |
| 1 1 . 4 . 5 | 移动 A d h o c 网络的入侵检测技术 | 2 8 4 |
| 1 1 . 4 . 6 | 移动 A d h o c 网络的信任管理机制 | 2 8 4 |
| 1 1 . 5 | 小结 | 2 8 5 |

习题 2 8 5

参考文献 2 8 7

版权说明：本站所提供下载的 P D F 图书仅提供预览和简介，请支持正版图书。

信息来源：信息安全导论 t x t e p u b k i n d l e 下载 电子书 2 0 2 4 - 书

信息安全导论

信息安全导论作者简介

李冬冬，北京电子科技学院副教授，长期从事网络安全、信息安全的教学和科研工作。主讲《信息安全技术》、《网络安全协议》、《信息安全素质教育》、《信息安全管理》等课程，教学效果优秀。主持和参与了出版教材两本、译著四本。获中共中央办公厅科技进步三等奖两项、北京市高等教育教学成果二等奖两项、学院教育教学成果奖一等奖六项、二等奖四项。

版权说明：本站所提供下载的 P D F 图书仅提供预览和简介，请支持正版图书。

信息来源：信息安全导论 [t x t](#) [e p u b](#) [k i n d l e](#) 下载 电子书 2 0 2 4 - 书

信息安全导论

信息安全导论其它

编辑推荐

全书采用理论与实践相结合的方式，详细介绍了信息安全的基本概念、身份认证技术、授权与访问控制技术、操作系统安全、网络攻击与防御技术、网络边界防御技术、入侵检测技术、恶意代码及其防范、网络安全协议、W e b 应用安全、无线网络安全等内容。

书籍介绍

全书介绍了信息安全的基本概念、身份认证技术、授权与访问控制技术、操作系统安全、网络安全协议、网络攻击技术、边界防御技术、入侵检测技术、W e b 安全、无线安全等内容。每章均配有习题，包括选择题、填空题、论述题和实践题，帮助读者巩固本章所学理论知识，并进行实践尝试。

版权说明：本站所提供下载的 P D F 图书仅提供预览和简介，请支持正版图书。

信息来源：信息安全导论 t x t e p u b k i n d l e 下载 电子书 2024 - 书

尾页

版权说明

本站所提供下载的P D F图书仅提供预览和简介，请支持正版图书。

更多精彩内容请访问：[信息安全导论](#) [t x t](#) [e p u b](#) [k i n d l e](#) [下载](#) [电子书](#) 2

P [信息安全导论](#) [p d f](#) [下载地址](#) [网盘](#) [在线](#) 2 0 2 4

E [信息安全导论](#) [e p u b](#) [下载地址](#) [网盘](#) [在线](#) 2 0 2 4

A [信息安全导论](#) [a z w 3](#) [下载地址](#) [网盘](#) [在线](#) 2 0 2 4

M [信息安全导论](#) [m o b i](#) [下载地址](#) [网盘](#) [在线](#) 2 0 2 4

W [信息安全导论](#) [w o r d](#) [下载地址](#) [网盘](#) [在线](#) 2 0 2 4

T [信息安全导论](#) [t x t](#) [下载地址](#) [网盘](#) [在线](#) 2 0 2 4