

<<网络安全与信息保障>>

图书基本信息

书名：<<网络安全与信息保障>>

13位ISBN编号：9787302268642

10位ISBN编号：7302268649

出版时间：2012-1

出版时间：清华大学出版社

作者：仇建平

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>

## <<网络安全与信息保障>>

### 前言

路由与交换型网络基础与实践教程随着计算机网络技术的飞速发展，互联网已经深入到社会的各个方面，它人们对人们的工作方式、生活方式甚至思维方式都产生了巨大的影响，因此，可以说互联网已经成为现代人生活中不可缺少的一部分。

但是，人们在享受互联网所带来愉悦的同时，也不可避免地受到一系列网络及信息安全问题的困扰：网络上充斥虚假信息、非法信息，病毒日益猖狂，黑客攻击无孔不入等，这些都严重危及到个人、企事业单位乃至国家的信息安全。

研究如何采取有效的方法来保护重要信息变得越来越有必要，本书便是在这样一个大背景下编撰而成的。

本书立足于当前网络安全与信息保障的具体实践，深刻而全面地反映了现代网络安全与信息保障的新理论、新方法、新成果。

本书在内容的选择上注重学术性、实用性、创新性与可获得性，同时也综合考虑了不同学校和不同单位的教学实际，力求内容典型、精炼、新颖，具有代表性和可操作性。

创造性地将网络安全与信息保障工具融进了传统教学中，充分揭示了网络安全与信息保障的新进展；系统而全面地介绍了常用的网络安全与信息保障理论；集中介绍了网络安全与信息保障实践，相关实验的介绍基本涵盖了网络安全与信息保障有关的内容；系统而全面地阐述了网络攻防的途径与方法，重点介绍了网络攻防的实例；系统而全面地总结了网络安全与信息保障的国内外进展。

其中，网络攻防是国内相近专著和教材中所未包含的全新内容。

在全面总结当前国内外网络安全与信息保障和利用教材、专著、教学实践经验的基础上，提炼出基本适合于网络安全与信息保障教学、能力教育与培养的核心内容，在教学实践基础上增加了创新性的新内容，相关内容丰富了网络安全与信息保障理论，对于增强学生的相关能力，提高综合素质都有重要的意义。

因此，本书作为一本以信息安全为核心的教材，从实用和可获得性理论的角度出发专门介绍网络攻防的方法和技巧，这是国内对网络安全与信息保障课教学实践和教材使用上的大胆创新，对于全面提高信息管理、计算机科学与技术专业学生的信息素质和综合利用相关工具进行信息安全管理的能力、增强学生的信息安全意识和管理信息能力都有重要的现实意义和深远影响。

编者 2011年9月

## <<网络安全与信息保障>>

### 内容概要

《21世纪高等院校计算机网络工程专业规划教材：网络安全与信息保障》全面介绍了网络安全与信息保障的基本框架，网络安全与信息保障的基本理论，以及网络安全与信息保障方面的管理、配置和维护，具有如下特点。

内容先进，结构新颖。

书中吸收了国内最先进的新技术、新知识、新方法和国际通用准则，注重科学性、先进性、操作性。

?注重实用的特色。

坚持“实用、特色、规范”的原则，突出实用及素质能力的培养，在内容安排上，通过大量案例将理论知识与实际应用有机结合。

资源配套。

《21世纪高等院校计算机网络工程专业规划教材：网络安全与信息保障》提供配套的电子教案，并有辅助的实验，内容包括学习指导、实验教学、练习测试和课程设计等。

《21世纪高等院校计算机网络工程专业规划教材：网络安全与信息保障》可作为本科院校计算机类、信息类、电子商务类和管理类专业的信息安全相关课程的教材，也可作为培训及参考用书，还可作为高职院校相关专业师生的选修教材。

## &lt;&lt;网络安全与信息保障&gt;&gt;

## 书籍目录

第1章 网络安全与信息保障概述1.1 引言1.1.1 信息安全概述1.1.2 对信息的安全需求的理解1.1.3 网络安全潜在威胁及不安全因素1.2 网络安全与信息保障技术的发展1.2.1 网络安全体系结构1.2.2 主要的安全服务1.2.3 网络安全服务与网络层次关系1.2.4 网络安全标准1.2.5 安全策略的重要性1.3 信息安全管理模型 (SSE-CMM) 1.3.1 背景1.3.2 SSE CMM的益处1.3.3 SSE CMM项目1.3.4 与其他工程和研究项目的关系1.4 网络攻击简介1.4.1 网络攻击1.4.2 网络攻击概述1.4.3 网络安全技术1.5 实例分析——ARP攻击及欺骗1.5.1 ARP攻击行为1.5.2 针对PC的ARP欺骗行为1.5.3 针对网关的ARP欺骗行为第2章 防火墙技术2.1 防火墙概述2.2 防火墙的功能2.3 防火墙的分类2.4 防火墙的体系结构2.5 防火墙的实现技术2.6 防火墙的缺点第3章 PKI技术3.1 PKI概述3.2 密码学基础回顾3.3 密码攻击3.4 密码算法及其分类3.5 RSA密码算法3.6 认证基础3.6.1 数字签名3.6.2 身份认证3.6.3 验证主体身份3.7 认证协议3.7.1 基于口令的认证3.7.2 基于对称密码的认证3.7.3 基于公钥密码的认证3.7.4 零知识身份认证3.8 PKI及数字证书3.8.1 PKI概述3.8.2 PKI体系3.9 SSL3.9.1 SSL协议概述3.9.2 SSL记录协议3.9.3 SSL握手协议第4章 VPN技术4.1 VPN概述4.1.1 VPN关键技术4.1.2 VPN的分类4.1.3 虚拟专用网的工作原理4.2 IPsec与VPN实现4.2.1 IPsec概述4.2.2 封装安全载荷 (ESP) 4.2.3 验证头 (AH) 4.2.4 Internet密钥交换第5章 入侵检测5.1 入侵检测概述5.1.1 IDS存在与发展的必然性5.1.2 入侵检测的概念5.2 入侵检测系统的基本结构5.3 入侵检测的分类5.3.1 根据采用的技术分类5.3.2 根据其监测的对象是主机还是网络分类5.3.3 根据工作方式分类5.4 入侵检测方法5.4.1 基本概念5.4.2 入侵检测技术检测方法5.5 入侵系统的分析方式5.6 入侵检测发展5.6.1 入侵技术的发展与演化5.6.2 入侵检测技术的主要发展方向第6章 病毒防护技术6.1 病毒防护技术概述6.2 计算机病毒6.3 VBS病毒特征分析6.3.1 病毒感染特征简介6.3.2 病毒感染实例6.3.3 特征代码分析6.3.4 病毒清除6.4 冲击波病毒特征分析6.4.1 冲击波病毒特征简介6.4.2 病毒感染实例6.4.3 病毒样本反汇编分析6.4.4 病毒跟踪6.4.5 深入分析6.5 单机CIH病毒特征分析第7章 安全策略7.1 安全策略概述7.2 组织的安全7.2.1 信息安全基础7.2.2 第三方访问的安全性7.3 外包7.4 工作责任中的安全因素7.4.1 用户培训7.5 实际和环境的安全7.5.1 安全区域7.5.2 设备的安全7.6 通信与操作管理7.6.1 操作程序和责任7.6.2 系统规划与验收7.7 访问控制7.7.1 访问控制策略7.7.2 用户访问管理7.7.3 用户责任7.7.4 网络访问控制7.7.5 操作系统访问控制7.7.6 应用程序访问控制7.7.7 监控系统的访问和使用7.7.8 移动计算和远程工作7.8 系统开发与维护7.9 业务连续性管理7.10 符合性第8章 大型企业局域网安全解决方案8.1 方案概述8.2 网络概况8.2.1 网络概述8.2.2 网络结构8.2.3 网络应用8.2.4 网络结构的特点8.3 网络系统安全风险8.4 安全需求与安全目标8.5 网络安全方案总体设计8.6 网络安全体系结构8.6.1 物理安全8.6.2 网络安全8.6.3 系统安全8.6.4 信息安全8.6.5 应用安全8.6.6 安全管理第9章 实验实验一 使用Ethereal检测工作在混杂模式下的网卡实验二 net命令入侵实例实验三 通过139端口远程重新启动Windows服务器实验四 使用tracert命令检测路由和拓扑结构信息实验五 使用WS\_PingPropack进行网络检测和扫描实验六 用ping和tracert来判断网络操作系统类型实验七 Windows2000配置启用系统审核实验八 使用Sniffer工具进行TCP/IP分析实验九 ISA防火墙应用实验十 Windows2000的文件加密实验十一 PGP实验实验十二 配置Windows2000Server入侵监测实验十三 SessionWall入侵检测参考文献

## &lt;&lt;网络安全与信息保障&gt;&gt;

## 章节摘录

版权页：插图：信息和支持进程、系统以及网络都是重要的业务资产。

为保证组织富有竞争力，保持现金流顺畅和组织赢利，以及遵纪守法和维护组织的良好商业形象，信息的保密性、完整性和可用性是至关重要的。

各个组织及其信息系统和网络所面临的安全威胁与日俱增，来源也日益广泛，包括利用计算机欺诈、窃取机密、恶意诋毁破坏等行为，以及火灾或水灾。

危害的来源多种多样，如计算机病毒、计算机黑客行为、拒绝服务攻击等，这些行为呈蔓延之势、用意更加险恶，而且手段更加复杂。

组织对信息系统和服务的依赖意味着自身更容易受到安全威胁的攻击。

公共网络与专用网络的互联以及对信息资源的共享，增大了对访问进行控制的难度。

分布式计算尽管十分流行，但降低了集中式专家级控制措施的有效性。

很多信息系统在设计时，没有考虑到安全问题。

通过技术手段获得安全保障十分有限，必须辅之以相应的管理手段和操作系统才能得到真正的安全保障。

确定需要使用什么控制措施需要周密计划，并对细节问题加以注意。

作为信息安全管理的最基本要求，组织内所有的雇员都应参与信息安全管理。

信息安全管理还需要供应商、客户或股东的参与。

也需要参考来自组织之外的专家建议。

如果在制定安全需求规范和设计阶段时就考虑到了信息安全的控制措施，那么信息安全控制的成本会很低，并更有效率。

1.网络安全潜在威胁计算机网络所面临的威胁大体可分为两种：一是对网络中信息的威胁；二是对网络中设备的威胁。

影响计算机网络的因素很多，有些因素可能是有意的，也可能是无意的；可能是人为的，也可能是非人为的；也有可能是外来黑客对网络系统资源的非法使用。

目前，归结起来网络安全所面临的主要潜在威胁有以下几方面。

(1) 信息泄密。

主要表现为网络上的信息被窃听，这种仅窃听而不破坏网络中传输信息的网络侵犯者称为消极侵犯者。

(2) 信息被篡改。

这就是纯粹的信息破坏，这样的网络侵犯者称为积极侵犯者。

积极侵犯者截取网上的信息包，并对之进行更改使之失效，或者故意添加一些有利于自己的信息起到信息误导的作用。

积极侵犯者的破坏作用最大。

(3) 传输非法信息流。

用户可能允许自己同其他用户进行某些类型的通信，但禁止其他类型的通信，如允许电子邮件传输而禁止文件传送。

<<网络安全与信息保障>>

编辑推荐

《21世纪高等院校计算机网络工程专业规划教材:网络安全与信息保障》内容包括网络安全概述、网络安全与信息加密技术概述、数字签名和认证技术、信息隐藏技术等。

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>