

<<网络安全技术及实训>>

图书基本信息

书名：<<网络安全技术及实训>>

13位ISBN编号：9787300164014

10位ISBN编号：7300164013

出版时间：2013-1

出版时间：童均、陈学平 中国人民大学出版社 (2013-01出版)

作者：童均，陈学平 著

页数：313

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>

## <<网络安全技术及实训>>

### 前言

本书依托中国电子教育学会高职高专计算机类专业2012年教学研究规划课题“高职计算机网络专业人才培养模式创新与实践”（课题编号：CESE22012-24），全面介绍了网络安全的基本框架、网络安全的基本理论以及交换机、路由器、防火墙、无线网络的安全。

本书注重实践技能的培养，以实训为依托，深入浅出地讲解理论知识的应用，因此既可作为高等院校计算机及相关专业的教材，也可作为计算机网络安全类的技术参考书或培训教材。

本书从实战出发，以应用为目的，防范手段为重点，理论讲述为基础，避免了传统网络安全教材理论过多、实用性不强的问题，紧密跟踪网络安全领域最新问题和技术运用。

本书的主要内容如下：  
第1章网络安全概述。  
主要介绍了网络安全的特征、现状，网络攻击手段，网络安全分析和网络安全防范措施，同时设置了3个实训来强化技能。

第2章操作系统安全。  
主要介绍了用户账号安全、文件访问安全、端口安全与防范、软件安全、注册表安全、系统日志的安全审计、系统备份与恢复等内容，同时设置了7个实训来强化实践技能。

.....

## <<网络安全技术及实训>>

### 内容概要

《全国高等院校计算机职业技能应用规划教材：网络安全技术及实训》从网络系统安全管理和应用的角度出发，重点介绍网络安全技术及其应用的各个方面，各章在介绍网络安全技术后均配以相应的实践内容或应用实例，体现培养读者网络安全及管理技术的应用能力和实践操作技能的特色。

《全国高等院校计算机职业技能应用规划教材：网络安全技术及实训》对原理、技术难点介绍适度，将理论知识{和实际应用紧密地结合在一起，典型实例的应用性和可操作性强，便于学生学习和实践，内容安排合理，重点突出，文字简明，语言通俗易懂。

《全国高等院校计算机职业技能应用规划教材：网络安全技术及实训》可作为普通高校计算机、通信、信息安全等专业学生的网络安全实训教材，也可作为网络管理人员、网络工程技术人员、信息安全管理人员以及对网络安全感兴趣的读者的参考书。

## &lt;&lt;网络安全技术及实训&gt;&gt;

## 书籍目录

第1章 网络安全概述 1.1 网络安全的特征 1.2 网络安全现状 1.3 网络攻击手段 1.4 网络安全分析 1.5 网络安全防范措施 1.6 实训1—1：网络窃听 1.7 实训1—2：冰河木马远程控制 1.8 实训1—3：利用IPC漏洞进行远程攻击 习题第2章 操作系统安全 2.1 用户账号安全 2.1.1 密码策略 2.1.2 账户锁定策略 2.1.3 密码认证方式选择 2.1.4 实训2—1：Windows的账号安全性 2.2 文件访问安全 2.2.1 NTFS概述 2.2.2 实训2—2：NTFS安全权限设置 2.3 端口安全与防范 2.3.1 端口的重要性 2.3.2 端口的分类 2.3.3 端口的查看方法 2.3.4 端口攻击的防范对策 2.3.5 实训2—3：配置IP安全策略关闭端口 2.4 软件安全 2.4.1 软件限制策略 2.4.2 软件限制策略在操作系统安全中的应用 2.4.3 实训2—4：利用软件限制策略限制客户端安装和运行软件 2.5 注册表安全 2.5.1 注册表与网络安全 2.5.2 实训2—5：修改注册表实训网络安全 2.6 系统日志的安全审计 2.6.1 系统日志 2.6.2 安全审计 2.6.3 实训2—6：Windows 2003系统的安全审计 2.7 系统备份与恢复 2.7.1 备份模式 2.7.2 备份类型 2.7.3 实训2—7：操作系统的备份与恢复 习题第3章 网络加密与认证技术 3.1 加密技术 3.2 数字证书 3.2.1 授权机构 3.2.2 数字证书 3.2.3 数字签名 3.2.4 证书类型 3.2.5 证书格式 3.2.6 证书的申请、导入和导出 3.3 网络加密技术 3.3.1 网络加密技术分类 3.3.2 网络加密技术的应用 3.4 实训3—1：PGP实现文件加密和数字签名 3.5 实训3—2：加密算法DES和RSA的实现 3.6 实训3—3：证书服务器的安装和配置 3.7 实训3—4：配置web服务的SSL证书 3.8 实训3—5：邮件加密和数字签名 习题第4章 交换机安全配置 4.1 交换机端口安全概述 4.2 实训4—1：交换机的端口安全配置 4.3 实训4—2：ARP攻击与防御 4.4 IEEE 802.1 x安全网络接入 4.4.1 IEEE 802.1 x介绍 4.4.2 RADIUS服务介绍 4.4.3 基于IEEE 802.1 x认证系统的组成 4.4.4 实训4—3：RADIUS服务器的配置 4.5 实训4—4：配置交换机的保护功能 4.6 实训4—5：交换机端口镜像与监听 习题第5章 路由器安全配置 5.1 PPP协议简介 5.1.1 PPP链路建立过程 5.1.2 PPP认证方式 5.1.3 PPP协议的应用 5.1.4 实训5—1：配置PAP认证 5.1.5 实训5—2：配置CHAP认证 5.2 MD5认证技术 5.2.1 MD5认证介绍 5.2.2 实训5—3：配置RIP路由的MD5认证 5.2.3 实训5—4：OSPF邻居明文认证配置 5.2.4 实训5—5：OSPF的MD5认证配置 5.3 网络地址转换 5.3.1 网络地址转换简介 5.3.2 实训5—6：网络地址转换配置 5.4 访问控制列表 5.4.1 访问控制简介 5.4.2 实训5—7：配置访问控制列表限制网络流量 习题第6章 防火墙安全配置 6.1 防火墙简介 6.1.1 防火墙的概念 6.1.2 防火墙的作用 6.1.3 防火墙的类型 6.1.4 防火墙的基本特性 6.1.5 防火墙的代理服务 6.1.6 防火墙的优点 6.1.7 防火墙的功能 6.1.8 防火墙的架构 6.1.9 防火墙的三种配置 6.1.10 防火墙的发展史 6.2 锐捷RG—WALL160防火墙介绍 6.2.1 概述 6.2.2 防火墙硬件描述 6.2.3 防火墙的安装 6.2.4 通过CONSOLE串口命令进行管理 6.3 实训6—1：防火墙的基本配置 6.4 实训6—2：防火墙的地址转换 6.5 实训6—3：防火墙的访问控制策略配置 6.6 实训6—4：配置客户端认证 6.7 实训6—5：使用防火墙防止“死亡之ping”攻击 6.8 实训6—6：使用防火墙保护服务资源 习题第7章 虚拟专用网 7.1 虚拟专用网简介 7.2 远程VPN 7.3 站点到站点的VPN 7.3.1 单向初始化连接 7.3.2 双向初始化连接 7.4 服务器的VPN配置 7.4.1 实训7—1：配置服务器的端到端IPSec VPN 7.4.2 实训7—2：配置服务器的远程IPSEC VPN 7.5 路由器的VPN配置 7.5.1 实训7—3：配置路由器的端到端IPsec VPN 7.5.2 实训7—4：配置路由器的远程VPN 7.6 锐捷VPN设备基础 7.6.1 VPN设备介绍 7.6.2 实训7—5：VPN设备基本配置 7.7 锐捷VPN虚拟专用网配置 7.7.1 实训7—6：配置VPN设备的端到端VPN 7.7.2 实训7—7：配置VPN设备的远程VPN 习题第8章 无线网络安全 8.1 无线局域网安全技术 8.2 实训8—1：锐捷无线交换机的基本配置 8.3 锐捷无线交换机的安全配置 8.3.1 实训8—2：无线网络的WEP认证 8.3.2 实训8—3：无线网络的MAC认证 8.3.3 实训8—4：无线网络的802.1 x认证 8.3.4 实训8—5：无线网络的Web认证 8.4 无线路由器的安全配置 8.4.1 实训8—6：无线路由器的网络连接 8.4.2 实训8—7：设置网络密钥 8.4.3 实训8—8：禁用SSID广播 8.4.4 实训8—9：禁用DHCP 8.4.5 实训8—10：启用MAC地址、IP地址过滤 习题第9章 入侵检测系统 9.1 入侵检测系统简介 9.2 使用sessionwall监测ping flooding 习题参考文献

章节摘录

1.后门程序 当程序员设计一些功能复杂的程序时，一般采用模块化的程序设计思想，将整个项目分割为多个功能模块，分别进行设计、调试，这时的后门就是一个模块的秘密入口。在程序开发阶段，后门便于测试、更改和增强模块功能。正常情况下，完成设计之后需要去掉各个模块的后门，不过有时由于疏忽或者其他原因（如将其留在程序中，便于日后访问、测试或维护）后门没有去掉，一些别有用心的人会利用穷举搜索法发现并利用这些后门，然后进入系统并发动攻击。

2.拒绝服务 拒绝服务又叫DDOS攻击，它是使用超出被攻击目标处理能力的大量数据包消耗可用系统、带宽资源，最后致使网络服务瘫痪的一种攻击手段。作为攻击者，首先需要通过常规的黑客手段侵入并控制某个网站，然后在服务器上安装并启动一个可由攻击者发出的特殊指令来控制进程，攻击者把攻击对象的IP地址作为指令下达给进程的时候，这些进程就开始对目标主机发起攻击。这种方式可以集中大量的网络服务器带宽，对某个特定目标实施攻击，因而威力巨大，顷刻之间就可以使被攻击目标带宽资源耗尽，导致服务器瘫痪，比如1999年美国明尼苏达大学遭到的黑客攻击就属于这种方式。

3.网络监听 网络监听是一种监视网络状态、数据流以及网络上传输信息的管理工具，它可以将网络接口设置在监听模式，并且可以截获网上传输的信息，也就是说，当黑客登录网络主机并取得超级用户权限后，若要登录其他主机，使用网络监听可以有效地截获网上的数据，这是黑客使用最多的方法，但是，网络监听只能应用于物理上连接于同一网段的主机，通常被用做获取用户口令。

.....

## <<网络安全技术及实训>>

### 编辑推荐

童均、陈学平编著的《网络安全技术及实训》注重实践技能的培养，以实训为依托，深入浅出地讲解理论知识的应用，因此既可作为高等院校计算机及相关专业的教材，也可作为计算机网络安全类的技术参考书或培训教材。

本书从实战出发，以应用为目的，防范手段为重点，理论讲述为基础，避免了传统网络安全教材理论过多、实用性不强的问题，紧密跟踪网络安全领域最新问题和技术运用。

<<网络安全技术及实训>>

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>