

<<网络安全管理员>>

图书基本信息

书名：<<网络安全管理员>>

13位ISBN编号：9787111391128

10位ISBN编号：7111391128

出版时间：2012-8

出版时间：程庆梅、徐雪鹏 机械工业出版社 (2012-08出版)

作者：程庆梅 著

页数：116

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>

## <<网络安全管理员>>

### 内容概要

企业网络信息安全与安全维护、网络终端的安全隐患、网络设备安全管理、终端信任计划、私有数据公网传递安全，共5章，40个实训任务。

内容涉及现代网络安全管理员在实际工作中遇到的各种典型问题及其主流解决方案和实施步骤。

《网络安全管理员》是神州数码技能教学项目的配套指导教材，也是信息安全实践基地的指定训练教材。

本书还适用于各类职业院校相关专业课程师生；各中小企业网络管理员等。

## 书籍目录

前言 第1章 企业网络信息安全与安全维护 1.1信息安全现状 1.2信息安全隐患及安全策略 1.3信息安全与园区网安全维护 1.4加密与身份认证技术概述 1.4.1加密技术简介 1.4.2身份认证简介 1.5信息安全策略与法律法规 习题 第2章网络终端的安全隐患 2.1系统漏洞 2.1.1 Linux漏洞利用 实训1 Linux漏洞利用 2.1.2 Windows漏洞利用 实训2 Windows漏洞利用 2.2 MySQL数据库漏洞利用 实训3 MySQL数据库漏洞利用 2.3木马与病毒 实训4 “灰鸽子”木马的利用与防护 2.4拒绝服务攻击 实训5拒绝服务攻击 习题 第3章网络设备安全管理 3.1认识网络设备 3.1.1交换机的主要功能及实现 实训6交换机VLAN划分 实训7 VLAN跨交换机 实训8 VLAN间通信 实训9环路产生及生成树应用 3.1.2路由器的主要功能及实现 实训10路由器串口封装PPP协议 实训11路由器使用chap作PPP协议验证 实训12 IP地址设计及静态路由 实训13 RIP协议实现网间路由 实训14 OSPF协议实现网间路由 3.1.3防火墙的主要功能及实现 实训15防火墙模式选择及接口地址配置 实训16防火墙策略实施 实训17防火墙源地址转换实施 实训18防火墙目的地址转换 3.1.4无线AP的主要功能及实现 实训19无线AP和终端的对接 3.2安全维护交换机 3.2.1交换机console登录的安全计划 实训20交换机enable密码设置与验证 实训21密文保存交换机密码 3.2.2交换机网络管理方案的安全计划 实训22关闭交换机telnet服务 实训23关闭交换机http服务 实训24交换机SSH管理设置 3.3安全维护路由器 3.3.1路由器console登录的安全计划 实训25路由器登录用户设置 实训26路由器enable密码设置 3.3.2路由器网络管理方案的安全计划 实训27路由器设置telnet服务并增加安全主机 实训28路由器启用SSH管理方式 3.4安全维护防火墙 3.4.1增加管理主机 实训29设置维护防火墙的安全主机 3.4.2关闭ping回应 实训30关闭防火墙接口的ping回应功能 习题 第4章终端信任计划 4.1有线网络终端的接入安全保障 4.1.1交换机的访问管理和端口安全特性 实训31交换机访问管理实现 4.1.2802.1x交换机和认证服务器 实训32交换机802.1x接入设置 4.2无线网络终端的接入安全保障 4.2.1接入认证 实训33无线接入认证的配置与验证 4.2.2接入控制（MAC地址列表） 实训34无线设备的接入控制设置 4.2.3接入AP SSID隐藏 实训35无线AP的SSID隐藏设置 习题 第5章私有数据公网传递安全 5.1点到网的数据安全保障 5.1.1 VPDN概述 5.1.2 PPTP和L2TP VPDN的实现 实训36 PPTP VPN服务器的设置 实训37路由器与路由器之间VPDN通道建立 5.1.3 SCVPN的实现 实训38防火墙安全连接VPN的设置与验证 5.2网到网的数据安全保障 5.2.1 VPN概述 5.2.2 IPSec协议的实施 实训39路由器间IPSec VPN隧道的建立 实训40防火墙间IPSec VPN隧道的建立 习题

## 章节摘录

版权页：插图：现代密码技术发展至今20余年，出现了许多高强度的密码算法和密钥管理技术。数据安全技术也已由传统的只注重保密性转移到了保密性、真实性、完整性和可控性的完美结合，并且相继发展了身份认证、消息确认和数字签名技术。

所谓加密（Encryption）是指将一个信息（或称明文——Plaintext）经过加密钥匙（Encryption Key）及加密函数转换变成无意义的密文（Ciphertext），而接收方则将此密文经过解密函数、解密钥匙（Decryption Key）还原成明文。

这一概念是密码学的基础。

数据加密技术要求只有在指定的用户或网络下才能解除密码而获得原来的数据，这就需要给数据发送方和接收方一些特殊的信息用于加、解密，这就是所谓的密钥。

需要保护的原始信息称为明文，用密钥编码操作后得到的看上去没有意义的结果称为密文。

加密的优点是即使其他的控制机制（如密码、文件权限等）受到了攻击，入侵者窃取的数据仍是无用的。

密码技术的基本任务是使通常称为Alice和Bob的两个人在不安全的信道上进行通信，而他们的敌人Oscar不能理解他们正在通信的内容。

Alice打算发送给Bob的消息，我们称为明文。

明文的形式可以是任意的，在计算机领域里通常是二进制数据。

Alice用预先确定的密钥处理（加密）明文，得到密文，通过信道发送给Bob。

在信道上通过截听而能看到密文的Oscar由于不知道解密密钥，所以不能确定明文是什么，而知道解密密钥的Bob却能解密密文得到明文。

信息加密过程是由形形色色的加密算法具体实施的，密码设计的基本公理和前提是算法公开，系统的安全性仅依赖于密钥的保密性。

按照密钥使用方式不同来区分，可以将这些加密算法分为对称密钥密码算法（又称私有密钥算法）和非对称密钥密码算法（又称公钥密码算法）。

两种密码体制各有优缺点，适用于不同的加密需求和应用场合。

对于加密文件，一个常被讨论但又经常被误解的内容是加密强度。

什么构成了加密的强度，哪种级别的加密强度是被不同的安全需要所要求的，如何确定加密的有效强度？

加密强度主要取决于3个因素：1) 算法的强度。

除了尝试所有可能的密钥组合之外，任何数学方法都不能使信息被解密；应该使用工业标准的算法，因为它们已经被加密学专家测试过无数次：任何一个新的或个体的方法在被商业认证之前都不被信任。

。

2) 密钥的保密性。

数据的保密程度直接与密钥的保密程度相关，算法不需要保密，被加密的数据首先与密钥共同使用，然后通过加密算法加密。

3) 密钥强度。

根据加密和解密的应用程序，密钥的长度是由bit为单位。

在密钥的长度加上一位则相当于把可能的密钥的总数乘以2，简单地说构成一个任意给定长度的密钥的位的可能的密钥个数可以被表示为 $2^n$ ，因此一个40位密钥长度的算法将是240个可能的不同的密钥。



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>