

<<计算机网络安全>>

图书基本信息

书名：<<计算机网络安全>>

13位ISBN编号：9787302256373

10位ISBN编号：7302256373

出版时间：2011-8

出版时间：清华大学出版社

作者：冯昊

页数：245

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>

<<计算机网络安全>>

内容概要

本书结合作者多年的实际网络安全管理和教学经验，采取以能力为本位，先了解黑客的攻击技术，再做网管的编写思路，通过具体的网络安全案例，介绍了计算机网络安全、网络攻击与入侵、通信子网安全防范、网络服务器与主机的安全防范、病毒与木马的安全防范、电子商务的安全、计算机网络安全管理等实用内容，并配有大量习题和实训操作。

本书可作为高职高专计算机类相关专业的网络安全教材，也可作为网络安全的培训教材。

<<计算机网络安全>>

书籍目录

第1章 计算机网络安全概述

- 1.1 计算机网络安全的概念
- 1.2 计算机网络安全现状与安全威胁
 - 1.2.1 计算机网络安全现状
 - 1.2.2 计算机网络面临的安全威胁
- 1.3 保障计算机网络安全常用的措施
- 1.4 信息安全法律法规与违法案例
 - 1.4.1 信息安全法律法规
 - 1.4.2 信息安全违法案例

习题1

第2章 网络攻击与入侵途径

- 2.1 网络安全扫描
 - 2.1.1 端口与漏洞扫描
 - 2.1.2 用户密码暴力破解
- 2.2 IPC\$远程连接
 - 2.2.1 IPC\$简介
 - 2.2.2 IPC\$远程连接入侵步骤简介
 - 2.2.3 IPC\$连接的创建与管理
- 2.3 网络安全检查常用命令
 - 2.3.1 net命令
 - 2.3.2 nc命令
 - 2.3.3 at命令
 - 2.3.4 netsvc与sc命令
- 2.4 账户后门
 - 2.4.1 克隆系统账户
 - 2.4.2 创建隐藏账户
- 2.5 终端服务
 - 2.5.1 终端服务简介
 - 2.5.2 终端服务的远程开启与管理
- 2.6 清除日志
- 2.7 网络安全漏洞与网络安全
 - 2.7.1 安全漏洞简介
 - 2.7.2 Unicode漏洞攻击及防范
 - 2.7.3 SQL注入漏洞攻击及防范

习题2

- 实训2.1 利用IPC\$连接入侵主机
- 实训2.2 创设账户后门
- 实训2.3 远程开启和控制目标主机的终端服务
- 实训2.4 SQL注入攻击

第3章 通信子网安全防范

- 3.1 通信子网常用的安全措施
- 3.2 防火墙
 - 3.2.1 防火墙简介
 - 3.2.2 防火墙的分类
 - 3.2.3 防火墙的配置途径与配置策略

<<计算机网络安全>>

- 3.2.4 安装配置基于硬件的防火墙
- 3.2.5 利用三层交换机配置实现防火墙功能
- 3.2.6 利用Linux系统配置实现防火墙功能

3.3 入侵检测系统与防御系统

3.4 在汇聚层交换机配置报文过滤

- 3.4.1 配置策略
- 3.4.2 思科交换机ACL配置方法
- 3.4.3 华为或华三交换机ACL配置方法

习题3

实训3.1 安装配置基于硬件的防火墙

实训3.2 利用三层交换机配置实现防火墙功能

第4章 网络服务器与主机的安全防范

4.1 服务器硬件配置与安全

- 4.1.1 物理与环境安全
- 4.1.2 服务器硬件配置的基本要求
- 4.1.3 服务器系统安装与数据安全

4.2 服务器面临的主要安全威胁

4.3 保护服务器安全常用的措施

- 4.3.1 打补丁修复系统漏洞
- 4.3.2 安装反病毒和防火墙软件
- 4.3.3 修改注册表提升安全性
- 4.3.4 禁用或停用部分系统服务
- 4.3.5 严格管理用户账户与权限
- 4.3.6 开启账户策略和系统审核策略
- 4.3.7 Web与FTP服务器额外的安全设置

4.4 Web应用程序的安全措施

- 4.4.1 防止SQL注入攻击
- 4.4.2 合理分配数据库账户权限
- 4.4.3 使用加密技术和强密码保护账户安全
- 4.4.4 使用访问控制提升发布后台的安全性

4.5 用户主机的安全防范

习题4

实训4.1 Web服务器安全设置

实训4.2 强化网站发布系统的安全性

第5章 病毒与木马的安全防范

5.1 病毒与木马简介

5.2 使用360安全卫士查杀木马

5.3 使用光盘启动查杀病毒与木马

5.4 病毒与木马的手动清除

- 5.4.1 使用IceSword检查与终止进程
- 5.4.2 使用unlocker解锁文件
- 5.4.3 使用Autoruns查看自启动项目
- 5.4.4 使用SREng修复系统

习题5

实训5.1 使用360安全卫士清除木马或插件

实训5.2 手动清除病毒与木马

第6章 电子商务的安全

<<计算机网络安全>>

- 6.1 电子商务的安全要素
 - 6.2 电子商务安全的技术保障
 - 6.2.1 使用加密技术解决数据的机密性
 - 6.2.2 数字摘要与数字签名
 - 6.2.3 数字证书与认证中心
 - 6.2.4 时间戳
 - 6.2.5 SSL/TLS安全协议
 - 6.2.6 使用防火墙技术解决网络层的安全
 - 6.3 使用PGP软件加解密数据
 - 6.3.1 PGP简介
 - 6.3.2 安装与配置PGP
 - 6.3.3 使用PGP加解密数据
 - 6.4 安全Web服务器的配置与实现
 - 6.4.1 安全Web服务器简介
 - 6.4.2 安装配置CA证书服务器
 - 6.4.3 Web服务器证书的申请与安装
 - 6.4.4 客户端证书的申请与安装
- 习题6
- 实训6.1 使用PGP加解密数据
 - 实训6.2 配置使用安全Web服务器

第7章 计算机网络安全管理

- 7.1 网络流量监控
 - 7.1.1 使用PRTG进行流量监控
 - 7.1.2 使用MRTG进行流量监控
- 7.2 使用Sniffer捕包分析
 - 7.2.1 Sniffer简介
 - 7.2.2 安装Sniffer
 - 7.2.3 使用Sniffer进行捕包分析
- 7.3 网络内容审计

习题7

- 实训7.1 使用PRTG进行流量监控
- 实训7.2 使用Sniffer进行捕包分析

参考文献

<<计算机网络安全>>

章节摘录

版权页：插图：

<<计算机网络安全>>

编辑推荐

《计算机网络安全》为高职高专计算机任务驱动模式教材之一。

<<计算机网络安全>>

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>