

## <<入侵检测系统实训教程>>

### 图书基本信息

书名：<<入侵检测系统实训教程>>

13位ISBN编号：9787111378853

10位ISBN编号：7111378857

出版时间：2012-5

出版时间：程庆梅、徐雪鹏 机械工业出版社 (2012-05出版)

作者：程庆梅 著

页数：85

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>

## <<入侵检测系统实训教程>>

### 内容概要

《教育部师资实践基地系列教材·信息与网络安全·神州数码校企合作技能训练系列：入侵检测系统实训教程》主要围绕神州数码网络入侵检测系统的安装部署以及各种典型应用展开。

全书共设计四个部分：IDS系统部署、查询工具的安装与使用、安全响应策略的配置及联动、常见攻击模拟，共十一个独立的实训任务。

本书是典型的实训教程，以实际工作内容为依托，形成典型的实训工作设计，按照一般学习思维活动的特点进行系统化编排和整理。

本书的主体内容均包含：任务目的、任务设备及要求、任务步骤、任务思考与练习，既保证了实训的可操作性，又对实训后的理论提升创造了空间。

本书读者对象为：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。

## <<入侵检测系统实训教程>>

### 书籍目录

前言 导读 单元1 IDS系统部署 任务1 IDS传感器的安装配置 任务2 IDS软件支持系统的安装配置 任务3 IDS监控与管理环境搭建 单元2 查询工具的安装与使用 任务1 IDS查询工具及报表工具的安装 任务2 使用报表工具查看模拟攻击 单元3 安全响应策略的配置及联动 任务1 IDS联动插件的安装与使用 任务2 在网络内部模拟攻击行为, 观察并分析IDS系统和防火墙的响应 单元4 常见攻击模拟 任务1 安全攻击——特洛伊木马 任务2 安全攻击任务网络监听sniffer 任务3 安全攻击任务——扫描器+口令探测 任务4 安全攻击任务——拒绝服务攻击

## <<入侵检测系统实训教程>>

### 章节摘录

版权页：插图：单元1 IDS系统部署 学习目标 1.了解IDS的各项配置，明确管理环境搭建和不同管理方法之间的差异 2.掌握IDS控制台的搭建步骤，控制软件生成数据的观察分析与使用 重点及难点 IDS——入侵检测系统是一种安全设备，它依照一定的安全策略，通过软、硬件，对网络、系统的运行状况进行监视，尽可能发现各种攻击企图、攻击行为或者攻击结果，以保证网络系统资源的机密性、完整性和可用性。

2.IDS的重要性以及管理环境的搭建与备份 IDS是防火墙以后的第二道安全防线，可以有效地防止防火墙和操作系统与应用程序的设定不当，监测内部使用者的不当行为，了解和观察攻破第一道防线防火墙入侵者的行为意图，并收集入侵方式的资料，以及时阻止恶意的网络行为。

只有对DCNIDS - 1800控制台进行多方位地了解以及熟练地使用才可以更加有效地防止入侵，以及时地想出应对策略。

对于安全设备而言，设备的配置文件被妥善地备份，将有助于在安全事件发生后以最快的速度恢复网络的可用性。

通常设备的系统文件也需要进行及时的备份，这样可以保障系统文件丢失或者进行版本升级失败时，恢复系统的可用性。

合格的网络管理和维护人员，一定要对所有关键网络设备中的重要文件加以备份，才可以在需要的时候及时、有效地恢复网络的可用性。

知识补充 IDS探测器基本分为两类：基于网络的IDS和基于主机的IDS。

基于网络的IDS如同“超级”嗅探器，它们在TCP / IP层或者更底层监视流量，监测是否有已知的攻击。

基于主机的IDS采取不同的方法搜索攻击模式，其检测事件主要靠操作系统的日志，因此它不能检测到发生在网络层的攻击。

DCNIDS - 1800是基于网络的入侵检测系统。

无论是基于网络的还是基于主机的IDS都要在以下几个环节做好重要的准备：1) IDS监控及回应。

2) 事件的处理。

3) 犯案分析及数据保留。

4) 报告过程。

## <<入侵检测系统实训教程>>

### 编辑推荐

《入侵检测系统实训教程》给所有对学习计算机网络安全技术有兴趣的人士。所教授的技术和引用的案例都是神州数码推荐的设计方案和典型的成功案例。

## <<入侵检测系统实训教程>>

### 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>