

<<CCSP自学指南>>

图书基本信息

书名：<<CCSP自学指南>>

13位ISBN编号：9787115131966

10位ISBN编号：7115131961

出版时间：2005-1

出版时间：人民邮电出版社

作者：请买家自查

页数：555

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>

## &lt;&lt;CCSP自学指南&gt;&gt;

## 内容概要

《CCSP自学指南：Cisco安全入侵检测系统(CSIDS)(第2版)》是Cisco公司认可的自学教材，以Cisco IDS课程为基础详尽地介绍了Cisco入侵防护系统(IPS)的各个主要部分。

《CCSP自学指南：Cisco安全入侵检测系统(CSIDS)(第2版)》首先勾勒出了网络安全的基本轮廓，然后介绍了入侵检测和IDS体系、Cisco网络IDS配置、报警管理、病毒特征配置及响应的方法、主机入侵防护、Cisco IDS维护和故障排除、企业级IDS管理、企业级IDS监控和报告、Cisco威胁响应等。

由于Cisco IPS所能提供的功能正在不断演化发展，因此《CCSP自学指南：Cisco安全入侵检测系统(CSIDS)(第2版)》最后一章介绍了Cisco入侵防护系统即将具备的功能。

(这些功能很可能在《CCSP自学指南：Cisco安全入侵检测系统(CSIDS)(第2版)》出版时变成现实。

)《CCSP自学指南：Cisco安全入侵检测系统(CSIDS)(第2版)》附录部分提供了Cisco入侵防护解决方案配置的案例学习以及各章复习题答案。

《CCSP自学指南：Cisco安全入侵检测系统(CSIDS)(第2版)》可以作为CCSP认证考试的备考、复习材料使用。

对于维护和操作Cisco IDS系统的技术人员来说，《CCSP自学指南：Cisco安全入侵检测系统(CSIDS)(第2版)》也是一本出色的参考书。

## 作者简介

Earl carter已在计算机安全领域工作了8年之久。  
他在美国空军信息战中心工作时开始钻研计算机安全。  
Earl的主要任务是确保美国空军网络能够抵抗网络攻击。  
他于1998年加入Cisco，为Netranger与Netsonar从事IDS研究。  
Earl花了大约1年时间为Netranger编写特征，为Netsonar开发了软件模块。  
现在，他是隶属于咨询工程部的安全技术评估小组的成员。

他的职责包括对Cisco的各种产品进行安全评估，同时向Cisco其他小组提供咨询，以帮助加强Cisco产品的安全性。  
他已经评测了从PIX防火墙到Cisco callmanager等众多Cisco产品。  
目前，Earl 持有CCNA证书，并在努力取得安全CCIE证书。

## 书籍目录

第1章 对网络安全的需要1.1 安全威胁1.1.1 无组织的威胁1.1.2 有组织的威胁1.1.3 外部威胁1.1.4 内部威胁1.2 安全概念1.3 攻击的各个阶段1.3.1 设定攻击目标1.3.2 攻击前的侦察1.3.3 正式攻击1.4 攻击方法1.4.1 即兴攻击1.4.2 系统性攻击1.4.3 外科手术式打击1.4.4 耐心（慢）攻击1.5 网络攻击点1.5.1 网络资源1.5.2 网络协议1.6 黑客工具与技术1.6.1 使用侦察工具1.6.2 攻击网络中的薄弱点1.6.3 实施拒绝服务攻击技术1.7 小结1.8 复习题第2章 网络安全与Cisco2.1 保护网络安全2.1.1 加强认证2.1.2 建立安全边界2.1.3 通过虚拟专用网提供私密性2.1.4 漏洞修补2.2 监控网络安全2.2.1 人工监控2.2.2 自动监控2.3 检验网络安全2.3.1 使用安全扫描器2.3.2 进行专业安全评估2.4 提升网络安全2.4.1 留意安全新闻2.4.2 定期检查配置文件2.4.3 评估传感器的放置2.4.4 验证安全配置2.5 Cisco集成化语音、视频和数据（AVVID）体系结构2.5.1 Cisco AVVID体系结构2.5.2 Cisco AVVID的益处2.6 Cisco SAFE2.6.1 SAFE模块化蓝图2.6.2 SAFE的益处2.7 小结2.8 复习题第3章 入侵检测的概念3.1 入侵检测的定义3.2 IDS警报术语3.2.1 错误警报3.2.2 正确警报3.3 IDS触发器3.3.1 异常检测3.3.2 滥用检测3.3.3 协议分析3.4 IDS监控位置3.4.1 基于主机的IDS3.4.2 基于网络的IDS3.5 混合IDS3.5.1 优点3.5.2 缺点3.6 入侵检测响应技术3.6.1 TCP重置3.6.2 IP拦截3.6.3 记录3.6.4 访问限制3.7 入侵检测逃避技术3.7.1 泛洪3.7.2 分片3.7.3 加密3.7.4 迷惑3.7.5 TTL操作3.8 小结3.9 复习题第4章 Cisco入侵防护4.1 Cisco入侵检测系统（IDS）解决方案概述4.1.1 入侵防护4.1.2 积极防御4.1.3 深入防御4.2 Cisco IDS传感器4.2.1 网络传感器4.2.2 交换机传感器4.2.3 路由器传感器4.2.4 防火墙传感器4.2.5 主机代理4.3 Cisco威胁响应4.4 Cisco传感器管理4.4.1 Cisco IDS设备管理器4.4.2 Cisco IDS管理中心4.5 Cisco警报监控与报告4.5.1 Cisco IDS事件查看器4.5.2 Cisco IDS安全监控器4.6 部署Cisco IDS4.6.1 传感器的选择4.6.2 传感器的布放4.6.3 传感器部署的考虑4.6.4 传感器部署的情形4.7 小结4.8 复习题第5章 Cisco IDS体系结构5.1 以前的软件体系结构5.2 Cisco IDS 4.0软件体系结构5.2.1 cidWebServer5.2.2 mainApp5.2.3 logApp5.2.4 认证5.2.5 网络接入控制器（NAC）5.2.6 ctiTransSource5.2.7 sensorApp5.2.8 事件存储（Event Store）5.2.9 cidCLI5.3 Cisco IDS 4.0通信体系结构5.3.1 通信概述5.3.2 入侵检测应用程序接口5.3.3 远程数据交换协议5.4 用户账号和角色5.4.1 管理员5.4.2 操作员5.4.3 查看者5.4.4 服务5.5 小结5.6 复习题第6章 捕获网络数据流量6.1 数据流量捕获设备6.1.1 集线器6.1.2 网络分接头6.1.3 交换机6.2 交换机端口分析6.2.1 交换机端口分析（SPAN）端口术语6.2.2 传输控制协议（TCP）重置限制6.2.3 Catalyst 2900XL/3500XL交换机6.2.4 Catalyst 4000和6500交换机6.3 远程交换机端口分析6.4 虚拟局域网（Virtual Local-Area Network, VLAN）访问控制列表6.4.1 定义感兴趣的数据流量（Interesting Traffic）6.4.2 在CatOS上配置虚拟局域网访问控制列表（VACL）6.4.3 在Cisco互联操作系统（IOS）防火墙下配置VACL6.5 高级数据流量捕获6.6 小结6.7 复习题第7章 Cisco IDS网络传感器的安装7.1 IDS设备7.1.1 设备型号7.1.2 设备限制7.1.3 硬件注意事项7.2 IDS加速卡7.3 IDS设备命令行接口7.3.1 使用CLI7.3.2 用户角色7.3.3 CLI命令模式7.3.4 管理任务7.3.5 配置任务7.4 安装IDS设备7.4.1 从3.1版本升级到4.0版本7.4.2 初始化配置任务7.5 小结7.6 复习题第8章 Cisco IDS模块配置8.1 Cisco IDS模块（IDSM）8.1.1 第二代入侵检测系统模块（IDSM-2）技术指标8.1.2 关键特性8.1.3 IDSM同IDSM-2的比较8.2 IDSM-2配置8.2.1 IDSM-2初始化8.2.2 IDSM-2端口8.2.3 捕获数据流量8.2.4 IDSM-2数据流量流向8.3 Catalyst 6500交换机配置8.3.1 配置命令和控制端口8.3.2 监控数据流量8.3.3 中继配置任务8.3.4 管理任务8.4 故障排除8.4.1 IDSM-2状态发光二极管（LED）8.4.2 Catalyst 6500命令8.5 小结8.6 复习题第9章 Cisco IDS设备管理器与事件查看器9.1 Cisco IDS设备管理器9.1.1 系统要求9.1.2 安装Cisco IDS设备管理器9.1.3 Cisco IDS设备管理器接口结构9.1.4 访问IDS设备管理器（IDM）9.1.5 访问在线IDM帮助9.1.6 IDS设备管理器与Cookie9.1.7 IDS设备管理器与证书9.2 Cisco IDS事件查看器9.2.1 系统要求9.2.2 安装Cisco IDS事件查看器9.2.3 卸载Cisco IDS事件查看器9.2.4 启动Cisco IDS事件查看器9.2.5 指定使用IDS设备监控9.2.6 配置过滤器9.2.7 配置视图9.2.8 查看事件数据9.2.9 使用警报9.2.10 网络安全数据库（NSDB）9.2.11 配置首选项9.2.12 配置应用程序设置9.2.13 数据库管理9.3 小结9.4 复习题第10章 传感器配置10.1 在IDS传感器管理中心中添加传感器（IDS MC）10.1.1 传感器组10.1.2 独立传感器10.2 配置网络设置10.3 配置允许主机10.4 远程访问10.5 安全Shell（SSH）属性10.5.1 定义授权密钥10.5.2 生成新的主机密钥10.5.3 配置SSH已知主机密钥10.6 证书管理10.6.1 信任主机证书10.6.2 产生主机证书10.6.3 查看服务器证书10.7 配置时间10.7.1 设置时间10.7.2 配置时区10.7.3 配置NTP服务器10.7.4 配置夏令时10.7.5 修正时间10.8 添加用

户10.9 管理任务10.9.1 查看系统信息10.9.2 查看诊断信息10.9.3 重新启动传感器10.10 小结10.11 复习题  
第11章 特征配置第12章 特征响应第13章 Cisco IDS警报与特征第14章 主机入侵防护第15章 Cisco IDS维护与故障排除第16章 企业级IDS管理第17章 企业级IDS监控和报告第18章 Cisco威胁响应第19章 Cisco入侵防护系统预计功能附录A Cisco入侵防护解决方案调整：案例研究附录B 复习题答案术语表

## 媒体关注与评论

理解Cisco IDS如何保护、监控和增强物理安全策略； 回顾基于网络和基于主机的安全技术； 回顾安全轮图的概念，并使用SAFE方案把安全性应用于AVVID； 安装和配置Cisco IDS，以监控网络，防范恶意攻击； 理解Cisco威胁响应技术的优点和工作原理； 应用报警特征，熟练掌握定制特征的方法； 使用传感器的管理平台，在网络中有效实施Cisco IDS； 深入理解Cisco安全代理的体系架构。

除了使用防火墙和其他网络安全装置来限制入侵者外，使用入侵检测和相应的防范措施也非常重要。

这也是一个完备的网络安全方案的重要组成部分。

Cisco入侵检测传感器和各类管理功能组合在一起协同工作，为网络提供检测、告知和自动关闭恶意网络行为等多项功能。

本书为您提供了深入的配置和部署信息，以构建可靠的、强大的入侵检测解决方案。

本书是Cisco公司认可的自学教材，提供了当前所使用的各类Cisco IDS的详实资料，帮助您掌握基于主机和基于网络各类IDS功能。

章节概述将把您快速地引入到学习中，配置实例将向您展示如何把IDS的功能淋漓发挥，而每章结尾的复习题将测试您的知识掌握程度。

无论您是需要一本CIDS传感器配置的参考手册，还是需要准备642-531考试，本书都将为您提供有效的帮助。

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>