

<<Cisco安全入侵检测系统>>

图书基本信息

书名：<<Cisco安全入侵检测系统>>

13位ISBN编号：9787115111609

10位ISBN编号：711511160X

出版时间：2003-2

出版时间：人民邮电出版社

作者：卡特

页数：618

字数：973000

译者：李逢天

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>

## <<Cisco安全入侵检测系统>>

### 内容概要

本书详细介绍了Cisco Secure IDS的各个方面，内容包括：网络安全介绍、入侵检测和CSIDS环境、CSIDS安装、报警管理和入侵检测特征、CSIDS配置、Cisco安全入侵检测控制器(CSIDD)、Cisco安全IDS新版本等。

本书的内容基于Cisco Secure IDS课程，同时引入IDS课程以外的一些信息，是Cisco Secure IDS课程的有益参考和补充，并且可以作为Cisco Secure IDS策略管理员考试的独立学习指导。

## <<Cisco安全入侵检测系统>>

### 作者简介

Earl Carter在计算机安全领域已有6年的工作经验。

在美国空军信息作战中心工作，他就开始学习计算机安全。

Earl负责美国空军网络的安全，防止网络攻击。

1998年他进入Cisco开始研究NetRanger（目前为Cisco安全IDS）和NetSonar（目前为Cisco安全扫描器）

Earl用约一年的时间定

## &lt;&lt;Cisco安全入侵检测系统&gt;&gt;

## 书籍目录

|                                  |                     |                       |                  |                          |                    |                |                               |                |              |                            |   |                            |                         |                                |                        |               |                            |                          |                                     |                                       |                    |                             |                                |                         |                    |         |           |
|----------------------------------|---------------------|-----------------------|------------------|--------------------------|--------------------|----------------|-------------------------------|----------------|--------------|----------------------------|---|----------------------------|-------------------------|--------------------------------|------------------------|---------------|----------------------------|--------------------------|-------------------------------------|---------------------------------------|--------------------|-----------------------------|--------------------------------|-------------------------|--------------------|---------|-----------|
| 第一部分 网络安全介绍 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(随机)攻击             | 1.4.2 系统性攻击             | 1.4.3 外科手术式打击(闪电攻击)            | 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            | 1.6.4 小结                       | 1.7 复习题                 |                    |         |           |
| 第2章 Cisco安全轮图                    | 2.1 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 通过虚拟专用网络提供私密性      | 2.1.4 漏洞修补         | 2.2 监视网络安全     | 2.2.1 人工监视                    | 2.2.2 自动监视     | 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 评估安全探测器的置放       | 2.4.4 核验安全配置  | 2.5 小结                     | 2.6 复习题                  |                                     |                                       |                    |                             |                                |                         |                    |         |           |
| 第二部分 入侵检测与CSIDS环境 第3章 入侵检测系统     | 3.1 IDS触发器          | 3.1.1 异常检测            | 3.1.2 滥用检测       | 3.2 IDS监测位置              | 3.2.1 基于主机的IDS     | 3.2.2 基于网络的IDS | 3.3 混合特性                      | 3.4 小结         | 3.5 复习题      | 第4章 Cisco安全IDS概述           | 4.1 系统功能和特性                                     | 4.2 探测器平台和模块               | 4.2.1 4200系列探测器         | 4.2.2 Catalyst 6000系列交换器的IDS模块 | 4.3 控制器平台              | 4.3.1 控制器平台特性 | 4.3.2 作为控制器平台的Cisco安全策略管理器 | 4.3.3 Cisco安全入侵检测控制器     | 4.3.4 控制器平台特性比较                     | 4.4 Cisco Secure IDS和邮局(PostOffice)协议 | 4.4.1 PostOffice协议 | 4.4.2 PostOffice特性          | 4.4.3 PostOffice标识符            | 4.4.4 PostOffice寻址方案    | 4.5 小结             | 4.6 复习题 |           |
| 第三部分 CSIDS安装 第5章 Cisco安全IDS探测器部署 | 第6章 Cisco安全策略管理器的安装 | 第7章 在CSPM内安装4200系列探测器 | 第四部分 报警管理和入侵检测特征 | 第8章 处理CSPM中的Cisco安全IDS警报 | 第9章 理解Cisco安全IDS特征 | 第10章 特征序列      | 第五部分 CSIDS配置 第11章 CSPM内的探测器配置 | 第12章 特征和入侵检测配置 | 第13章 IP拦阻配置  | 第14章 Catalyst 6000 IDS模块配置 | 第六部分 Cisco安全入侵检测控制器(CSIDD) 第15章 Cisco安全ID控制器的安装 | 第16章 配置文件管理工具(nrConfigure) | 第17章 Cisco IOS防火墙入侵检测系统 | 第七部分 Cisco安全IDS的新版本            | 第18章 计划的Cisco安全IDS增强特性 | 第八部分 附录       | 附录A 配置入侵检测：案例研究            | 附录B Cisco Secure IDS体系结构 | 附录C Cisco Secure IDS Director基本故障排除 | 附录D Cisco Secure IDS日志文件              | 附录E 高级技巧           | 附录F Cisco Secure IDS特征结构和实施 | 附录G Cisco Secure IDS特征和推荐的报警级别 | 附录H Cisco IOS防火墙IDS特征列表 | 附录I Cisco安全通信部署工作表 | 附录J 术语  | 附录K 复习题答案 |

<<Cisco安全入侵检测系统>>

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>