

<<深入剖析网络边界安全>>

图书基本信息

书名：<<深入剖析网络边界安全>>

13位ISBN编号：9787111124801

10位ISBN编号：7111124804

出版时间：2003-8

出版时间：机械工业出版社

作者：(美)Stephen Northcutt

页数：436

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>

<<深入剖析网络边界安全>>

内容概要

本书站在一个比较高的层次上，以纵深防御思想为主线，全面而系统地介绍了网络边界安全的方方面面。

全书包括四个部分和三个附录。

这四个部分依次从基础性的介绍逐步转向综合性的介绍，按照适合读者思路的方式进行组织编排。

第一部分“网络边界基础”介绍了一些与边界有关的基本知识和核心概念。

第二部分“边界的延伸”集中介绍了组成网络安全边界的附加部件。

第三部分“边界设计”阐述了如何进行良好的设计。

第四部分“边界安全评估方法”讲述了如何评估与检查已设计好的网络边界。

附录中包含了Cisco访问列表配置示例，讨论了密码术的基础知识，并对网络空隙机制进行了概述。

这是一本有关网络安全的中高级技术性指南，适合于已充分了解TCP/IP和相关技术的安全专业人员、系统管理员及网络管理员阅读。

<<深入剖析网络边界安全>>

作者简介

Stephen Northcutt是世界知名的安全专家，曾任美国国防部信息战专家。他创建了Shadow Intrusion Detection System、DoD Shadow小组、GIAC Security Certification Series和SANS Immersion Security Training教育系统。目前，他是SANS Institute的一名导师。

<<深入剖析网络边界安全>>

书籍目录

译者序前言第一部分 网络边界基础 第1章 边界安全基础 1 1.1 行业术语 1 1.2 纵深防御 4 1.3 实例分析：纵深防御的运转 12 1.4 小结 13 第2章 报文过滤 14 2.1 TCP/IP预备知识：报文过滤的工作原理 14 2.2 使用Cisco路由器做为报文过滤器 15 2.3 有效使用报文过滤设备 18 2.4 报文过滤器存在的问题 27 2.5 动态报文过滤与自反访问表 32 2.6 小结 35 2.7 参考资料 35 第3章 有状态防火墙 36 3.1 有状态防火墙的工作原理 36 3.2 状态的概念 37 3.3 有状态过滤和有状态检查 45 3.4 小结 54 3.5 参考资料 55 第4章 代理防火墙 56 4.1 基础知识 56 4.2 代理的类型 58 4.3 代理或应用网关防火墙 59 4.4 代理的协议问题 61 4.5 常见的代理件 63 4.6 小结 65 4.7 参考资料 66 第5章 安全策略 67 5.1 防火墙策略 67 5.2 策略的开发步骤 73 5.3 边界策略 78 5.4 小结 80 5.5 参考资料 81 第二部分 边界的延伸 第6章 路由器的作用 83 6.1 路由器作为边界设备 83 6.2 路由器作为安全设备 87 6.3 路由器加固 94 6.4 小结 105 6.5 参考资料 106 第7章 网络入侵检测 107 7.1 网络入侵检测基本原理 107 7.2 边界防御体系中网络IDS的作用 113 7.3 IDS感测器的放置 115 7.4 实例分析 119 7.5 小结 122 第8章 虚拟专用网 123 8.1 VPN基础知识 123 8.2 VPN的优缺点 126 8.3 IPSec基础知识 129 8.4 其他VPN协议：PPTP和L2TP 147 8.5 小结 151 8.6 参考资料 152 第9章 主机加固 153 9.1 安全级别 153 9.2 级别1：防止本地攻击的安全加固 154 9.3 级别2：抵御网络攻击的安全加固 158 9.4 级别3：抵御应用程序攻击的安全加固 163 9.5 其他加固方针 165 9.6 小结 166 第10章 主机防御部件 167 10.1 主机和边界 167 10.2 反病毒软件 170 10.3 以主机为中心的防火墙 174 10.4 基于主机的入侵检测 185 10.5 主机防御部件的难点 191 10.6 小结 193 10.7 参考资料 193 第三部分 边界设计 第11章 设计基础 195 第12章 资源隔离 212 第13章 软件结构 234 第14章 VPN集成 250 第15章 根据性能调整设计 267 第16章 实例设计 285 第四部分 边界安全评估方法 第17章 维护安全边界 301 第18章 网络日志分析 322 第19章 防御部件故障诊断 333 第20章 评估技术 362 第21章 攻击设计 383 第22章 纵深防御的重要性 405 第五部分 附录 附录A Cisco访问列表配置示例 419 附录B 密码术基础 428 附录C 网络空隙 432

<<深入剖析网络边界安全>>

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>