

<<Handening Network In>>

图书基本信息

书名：<<Handening Network Infrastructure (中文版) >>

13位ISBN编号：9787302160069

10位ISBN编号：7302160066

出版时间：2007-9

出版时间：清华大学

作者：努南

页数：474

字数：677000

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>

<<Hardening Network In>>

内容概要

“Hardening”系列是美国McGraw—Hill公司新近推出的又一套信息安全系列丛书，与久负盛名的“黑客大曝光”系列携手，为信息安全界奉献了一道饕餮大餐。

本书是“Hardening”系列成员之一，由资深安全专家wesley执笔，通过网段式系统强化教学法，从技术和管理制度两方面，详细介绍了网络基础设施的安全防护工作，对系统管理员容易疏忽或犯错的细节进行深入探讨，旨在帮助读者把网络系统建设成信息安全堡垒。

全书共分4大部分17章。

第1部分给出降低系统威胁的6个关键措施，是系统阻IE入侵的必要手段；第2部分则是本书的重中之重，系统讲述强化网络基础设施安全的具体方法和措施；第3部分告诫人们：不能一劳永逸，需要利用各种监摔技术持续监控系统，教会读者执行安全复查，管理环境变更；第4部分对加强网络基础设施防护的成本、员工培训、响应计划进行讨论，同类书中少见。

本书是负责安全保障工作的网络管理员和系统管理员的必读之书，也可作为信息管理员以及对计算机和网络安全感兴趣的人员的参考书。

<<Handening Network In>>

作者简介

作者: (美) 努南 (Noonan, W.J.) 著, 张辉 等

<<Handening Network In>>

书籍目录

第1部分 立即行动! 第1章 开门六件事 1.1 复查网络设计 1.2 安装防火墙 1.2.1 应用代理
1.2.2 有状态的数据包检测 / 过滤网关 1.2.3 混合防火墙 1.2.4 应该实现哪种防火墙 1.3 实
现访问控制列表 1.4 关闭不必要的功能和服务 1.5 实施病毒防护 1.6 保护无线连接的安全 1.7
小结第2部分 从全局出发——系统级的加强防护过程 第2章 制定安全策略 2.1 安全策略的作用
2.2 安全策略的组成 2.2.1 从何处开始 2.2.2 良好安全策略的特征 2.3 安全策略建议
2.3.1 加密策略 2.3.2 模拟 / ISDN策略 2.3.3 防病毒策略 2.3.4 审计、安全漏洞评估和风险
评估策略 2.3.5 拨号策略 2.3.6 DMZ策略 2.3.7 外网策略 2.3.8 无线通信策略
2.3.9 VPN策略 2.3.10 防火墙安全策略 2.3.11 路由器和交换机安全策略 2.3.12 远程访问
策略 2.3.13 口令策略 2.3.14 入侵检测 / 保护系统策略 2.3.15 内容过滤 / Internet策略
2.3.16 企业级监视策略 2.3.17 AuP策略 2.3.18 网络连接策略 2.3.19 网络文档策略 2.4
为什么安全策略会失效, 如何避免失效 2.4.1 将安全当作前进的障碍 2.4.2 安全是后天学
会的行为 2.4.3 安全不乏意外事件和情况 2.4.4 安全策略始终没有尽头 2.4.5 防止失败 2.5
小结 第3章 强化防火墙 3.1 基于硬件和基于软件的防火墙 3.1.1 强化远程管理 3.1.2
实现身份验证和授权 3.1.3 强化操作系统 3.1.4 强化防火墙的服务和协议 3.1.5 利用冗余
强化防火墙 3.1.6 强化路由协议 3.2 小结..... 第4章 用IDS/IPS强化网络安全 第5章 强
化VPN和远程拨号访问 第6章 强化路由器和交换机 第7章 用内容过滤保护网络安全 第8章 加
强WLAN网络连接的安全 第9章 实现AAA 第10章 通过网络管理加强网络安全 第11章 实施一
个安全的边界 第12章 实施一个安全的内部网络第3部分 绝不能一劳永逸 第13章 审计: 执行安
全复查 第14章 管理环境变更第4部分 如何成功地加强网络基础设施的防护 第15章 树立认知并
证明安全成本 第16章 解决员工和培训问题 第17章 事故响应

<<Handening Network In>>

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>