<<免费保护你的网络>>

图书基本信息

书名：<<免费保护你的网络>>

13位ISBN编号：9787030234131

10位ISBN编号：7030234138

出版时间：2009-1

出版时间：科学出版社

作者：西格伦

页数：296

<<免费保护你的网络>>

内容概要

本书作者根据自己丰富的安全领域的经验，详细介绍了如何利用免费的工具来保护网络安全，讨论了Nmap，Wireshark，Snort和Nessus等工具的使用方法，同时辅以大量的实例，深入阐述入侵检测系统、漏洞扫描、防火墙使用、事件日志等内容。
适用于任何对网络安全感兴趣的读者参考。
本书特色： 详细介绍利用Nmap Wirestark Snort和Nessus等工具免费实现最顶级的网络安全保护。
提供了入侵检测系统、漏洞扫描、防火墙配置及更多的实例研究。
参考网站包含几十个可运行脚本和工具。

作者简介

Eric Seagren，拥有CISA，CISSP-ISSAP，SCNP，CCNA，CNE-4，MCPP+I和MCSE-NT证书，有10年的计算机行业从业经验。
近8年来，他为一家“财富”前100强的金融领域的公司提供服务。
Eric的计算机职业生涯从接触Novell服务器开始，并且在一家休斯敦本地的小公司从事排除一般网络故障的工作。
由于他一直在金融服务行业工作，故职位和职责都得到稳步提升，职责包括服务器管理、灾难恢复、业务连续性协调员、千年虫修补、网络脆弱性评估和风险管理。
过去几年，他是一名IT构建师和风险分析师，设计并评估了安全的、可扩展的冗余网络。

<<免费保护你的网络>>

书籍目录

第一作者技术编辑第1章 免费安全产品的商业案例 引言 使用免费安全产品的成本 培训成本 硬件成本 咨询成本 无形成本 使用免费安全产品节省的费用 购买费用 维护费用 定制费用 免费产品与商业产品的比较 免费产品的优势 免费产品的劣势 测评单个产品 “卖”一个免费产品 通过做来“卖” 提出一个提案 小结 快速解决方案 常见问题第2章 保护边界 引言 防火墙的类型 防火墙的体系结构 屏蔽子网 单边的 真正的非军事区域 实施防火墙 硬件防火墙和软件防火墙 配置netfilter配置Windows防火墙 提供安全的远程访问 VPN访问的提供 远程桌面的提供 远程壳的提供 小结 快速解决方案 常见问题第3章 保护网络资源 引言 执行基本强化 定义策略 访问控制 认证 授权 审计 强化Windows系统 一般的强化步骤 使用Microsoft的组策略对象 强化Linux系统 一般强化步骤 使用Bastme强化脚本 使用SELinux 强化基础设备 修补系统 修补Windows系统 修补Linux系统 个人防火墙 Windows防火墙 Netfilter防火墙 配置TCP封装 提供反病毒和反间谍软件保护 反病毒软件 反间谍软件 加密敏感数据 EFS（加密文件系统） 小结 快速解决方案 常见问题第4章 配置入侵监测系统 引言 入侵监测系统 配置入侵监测系统 硬件要求 放置NIDS 在WindOWS系统上配置Snort 安装Snort 配置Snort选项 使用Snort GUI前端 在Linux系统上配置Snort 配置Snort选项 Snort的GUI前端应用 其他Snort插件 应用Oinkmastei 其他研究 效果演示 小结 快速解决方案 常见问题第5章 管理事件日志 引言 产生Windows事件日志 用组策略生成Windows事件日志 生成自定义的Windows事件日志项 收集Windows事件日志 分析Windows事件日志 创建Syslog事件日志 Wirldows syslog Linux syslog 在Windows和Linux系统上分析syslog日志 保护事件日志 确保保管链的安全 确保日志完整 应用知识 小结 快速解决方案 常见问题第6章 系统测试与审计 引言 详细开列资产 定位和识别系统 定位无线系统 文档 脆弱性扫描 Nessus X-Scan Microsoft基线安全分析仪 开源软件安全测试方法指南（OSSTMM） 小结 快速解决方案 常见问题第7章 网络报告和故障排查 引言 带宽利用率和其他度量的报告 分析数据的收集 理解SNMP 配置多路由流量图示器 配置MZL和Novatech trafficstatistic 配置PRTG通信量图示仪 配置Ntop 开启Windows主机上的SNMP 开启Linux主机上的SNMP 网络问题的排查 GUI嗅探器的使用 命令行嗅探器的使用 其他故障排除工具 Netcat tracetcp Netstat 小结 快速解决方案 常见问题第8章 安全是一个持续的过程 引言 补丁管理 网络基础设施 操作系统补丁 应用程序补丁 变更管理 变更引起中断 不充分的文档化会使问题恶化 变更管理策略 杀毒软件 反间谍软件 入侵监测系统 漏洞扫描 漏洞管理周期 角色和责任 渗透测试 获得高级管理者的支持 阐明要买的东西 策略审议 物理安全 CERT小组（计算机突发事件响应小组） 小结 快速解决方案 常见问题

章节摘录

第1章 免费安全产品的商业案例引言你也许正在寻找解决安全问题的省钱的方法，并且想对可用的免费工具有更多了解。
本书将介绍一些最好的免费产品。
在一些环境中，首倡并实现任何类型的安全措施都会使你陷入麻烦中，即使有最好的计划，也会产生问题。
本章将帮助获得所需要的支持，以便实施一个低成本的产品。
无论是对解决方案进行修改并需将修改后的解决方案卖给经理的人，还是需要明白一个特定的免费软件的真正含义的决策者，本章都有助于找到所需的安全产品。
本章将讨论免费产品的一些隐性成本，并且阐明这些产品所带来的后果；本章也将说明一个事实：在很多情况下，一个免费包和一个商业产品之间一对一的比较是不合理的。
有了所有的信息，就应该能够提出一个解决方案并以一些令人信服的商业数据来支持自己的洗择。
使用免费安全产品的成本至于安全产品，生活中没有什么事是免费的。
可能不用为一个安全产品本身付钱，但有关实施产品的费用(这点并不明显)也许就免不了了。
很多情况下，安全需要指定哪个产品合适。
如果没有一个可用的免费产品，则不得不使用商业产品了。
幸运的是，有很多高质量的免费产品可用。
后面章节的内容旨在以各种混合等级提供一系列产品。
如果未经充分了解和研究就急不可待地实施一个免费产品，则有可能会比购买一个商业产品花费更多。

<<免费保护你的网络>>

版权说明