<<开放资源安全工具实践>>

图书基本信息

书名：<<开放资源安全工具实践>>

13位ISBN编号：9787030235947

10位ISBN编号：7030235940

出版时间：2009-1

出版时间：科学出版社

作者：（美）奥尔德　等著，傅建明　等译

页数：436

前言

随着网络的迅速发展与普及，它给人们的生活带来了翻天覆地的变化。
网上冲浪、电子商务、远程会议、文件共享、电子办公等，无不给人们的生活和工作带来了快乐和便利。
然而伴随着网络的扩展，与之而来的是更多的安全问题，如账号密码泄露、机密文件被窃取、整个网络瘫痪导致业务失效、网络被攻击导致重要文件丢失，这些网络安全问题在大家充分享受网络便利的同时也告诫大家：网络安全问题不容忽失，否则可能导致难以弥补的损失。
考虑到商业安全解决方案不仅昂贵且缺乏灵活性等特性，本书重点介绍开源免费安全工具，并对它们的特性、适用场景以及详细的配置和使用技巧进行了详细说明，从而展示了众多可以立即免费获得的高灵活性、可配置的安全解决方案。
同时，本书从安全加固程序的起始环节展开，介绍了开源免费安全工具的方方面面，一步步引导读者利用这些工具提高网络的安全性，解决现有网络中遗存的安全隐患。
本书适合所有的网络管理员和系统管理员，对现今各种开源安全工具和安全解决方案进行了详尽介绍，同时针对各种安全隐患提出了许多可行的有效解决方案。
可以说，本书是迄今为止最权威、详尽、系统的安全工具使用手册，其中凝聚了作者从实践中总结出来的智慧结晶，相信读者一定可以从中受益颇多。
当然，不仅仅是网络管理员等专业人员，对于网络安全爱好者、对网络安全工具和技术关心的人乃至希望保障个人网络安全的读者来说，也同样能从本书中受益。
作者不仅对开源安全工具进行了详细介绍，同时对涉及网络安全的各种问题都进行了阐述，并结合实际给出了具体的解决方法，而且这些方法是作者长期工作的经验积累，相信读者也必能从中找到感兴趣的内容。
从内容方面看，本书可分为4个主要部分：第1～3章为第一部分，主要涉及系统的探测、网络边界和网络资源的保护，重点讨论了探测工具、防火墙的配置和使用，以及系统的加固技术；第4～6章为第二部分，涉及网络入侵检测，重点阐述了Snort的原理、安装以及具体使用；第7～9章为第三部分，涉及网络协议分析，重点剖析了Wireshark的原理、安装以及具体使用；第10～11章为最后部分，涉及其他开源安全工具，重点分析了其他网络嗅探和数据分析的工具、无线网络监控及入侵检测工具。
本书包含大量的工具软件截图和配置实例，图文并茂，能帮读者利用免费开源的安全工具快速直接解决安全问题。
可以毫不夸张地说，本书囊括了当前所有开源安全工具的使用技巧和相应的安全解决方案，必能成为解决安全问题的智囊宝典。
在本书翻译的过程中，得到了潘宣辰、潘谧、陈洋溢、乔伟、李珊珊、李萌萌、陶芬等同学的大力支持，他们结合自身实践经验为本书的翻译工作提供了大量的宝贵意见，在此我十分感谢他们的帮助。同时也希望我们的工作能给各位读者带来帮助。
由于译者的专业知识和外语水平有限，书中可能存在错误，敬请读者指正。

<<开放资源安全工具实践>>

内容概要

本书重点介绍开源免费安全工具，并且对其特性、适用范围及详细配置和使用技巧进行了详细说明，同时针对各种安全隐患提出了许多可行的有效解决方案。
同时，本书提供了大量的工具软件截图和配置实例，图文并茂，能帮助读者利用这些免费开源的安全工具快速直接地解决安全问题。
适合网络管理员及对网络安全工具和技术感兴趣的读者阅读参考。

作者简介

Raven Alder，网络安全设计和部署咨询公司IOActive的高级安全工程师，她专门从事大规模企业级安全咨询工作，推崇深度防御。
她主要设计大规模的防火墙和IDS系统，然后进行漏洞评估和渗透测试来确保这些系统处于最佳的工作状态。
此外她还兼任LinuxChix．org的网络安全讲师，并为Open Source Vulnerability Database检查密码方面的漏洞。
Raven住在西雅图，也是“ Nessus Network Auditing ”（Syngress Publishing，ISBN：1-931836-08-6）一书的作者之一。

<<开放资源安全工具实践>>

书籍目录

章节摘录

第1章 系统的测试与审计引言总有一天，我们需要识别自己网络上的所有系统。
尽管有非常严格的使用策略，但有时网络中还是会存在未经授权的系统。
这些系统可能是一直保持使用的“测试”系统，但在某些时候它们仅仅是存在于网络中并违反了使用策略的“流氓”（rogue）系统，也可能这些系统是由设备供应商提供的附加产品并由第三方部门管理。
当你面对一个不熟悉的环境，如一个新收购的公司或者对职位还不了解时，全面的网络检测就显得更为重要。
如果该网络所拥有的主机数目不多，那么这项工作不难完成。
但如果网络十分庞大，甚至分布在不同的地理位置，则访问所有主机是不切实际的，此时自动化的检测方法是更合理的方案。
本章将分析一些通用的探测／扫描工具，也包括针对特定服务的工具。
识别出网络上所有的系统后，下一步应当是确定这些系统的安全状态。
现有的一些自动安全扫描工具可以帮助完成这项任务，并检测出大量的已知的漏洞。
我们将示范如何配置和操作一些自动漏洞扫描器，并讨论如何使用Microsoft基准安全分析器（Microsoft Baseline Security Analyzer，MBSA），它可以扫描Microsoft系统并报告已发现的安全问题。
最后，除了使用漏洞扫描器软件外，还可以使用规范的安全测试方法来评估一个系统的安全性。
系统探测在理想状况下，你应该拥有连入公司网络的所有系统的描述文档，并且这些文档是100%准确和完整的。
对于有网络访问权限的人而言，他们是不会在没有任何文档说明和授权的情况下将一台系统连入网络的。
但我们都知道，“理想状况”是不存在的。
也许你有一个特殊的理由进行网络探测，或者并没有。
但无论如何，即使没有任何特殊的理由，也应该选择定期进行网络探测，这样可以成功地为网络上所有的设备生成文档化的许可，以确保它们遵守既定的策略。
主机探测审计也可以验证描述文档与网络的真实状况是否一致，路由器和交换机是否在适当位置等。
鉴于对主机系统进行物理定位的困难性，尤其是考虑无线接入设备越来越小型化，基于网络的探测比基于物理的探测将更加有效。

<<开放资源安全工具实践>>

编辑推荐

《开放资源安全工具实践》适合所有的网络管理员和系统管理员，对现今各种开源安全工具和安全解决方案进行了详尽介绍，同时针对各种安全隐患提出了许多可行的有效解决方案。
可以说，《开放资源安全工具实践》是迄今为止最权威、详尽、系统的安全工具使用手册，其中凝聚了作者从实践中总结出来的智慧结晶，相信读者一定可以从中受益颇多。
当然，不仅仅是网络管理员等专业人员，对于网络安全爱好者、对网络安全工具和技术关心的人乃至希望保障个人网络安全的读者来说，也同样能从《开放资源安全工具实践》中受益。
作者不仅对开源安全工具进行了详细介绍，同时对涉及网络安全的各种问题都进行了阐述，并结合实际给出了具体的解决方法，而且这些方法是作者长期工作的经验积累，相信读者也必能从中找到感兴趣的内容。

<<开放资源安全工具实践>>

版权说明