<<网络安全宝典>>

图书基本信息

书名：<<网络安全宝典>>

13位ISBN编号：9787302239390

10位ISBN编号：7302239398

出版时间：2010-11

出版时间：清华大学出版社

作者：科尔

页数：697

<<网络安全宝典>>

前言

网络技术使得信息资源可以高度共享，同时也使人们面临着巨大的安全风险。
黑客入侵事件和计算机病毒常有发生。
为此，各国政府、军队、企业和其他相关机构都越来越重视网络安全问题，并不断为解决网络安全问题而投入大量资金和精力。
《网络安全宝典（第2版）》是一本介绍网络安全相关知识和方法的经典书籍。
与前一版本相比，本书涵盖了网络安全的新技术、新方法和新手段，并尝试由被动安全向主动安全转变。
本书可以作为网络安全领域的综合教程，也可以作为实现网络安全的技术手册。
全书共分为7个部分共29章，各部分的内容如下：第1部分概述了网络安全现状；第1I部分介绍了信息系统安全基础；第1II部分讨论了主要操作系统和应用程序中存在的安全问题；第IV部分介绍了网络安全基础；第V部分介绍了与安全通信相关的最佳实践：第VI部分介绍安全威胁与响应；第VII部分将前面各部分内容融为一个综合解决方案，并展望了网络安全的未来。
本书内容丰富、全面、新颖，适用于信息安全领域的从业人员和在日常工作中需要应对各种网络安全问题的人员。
其中深入探讨的问题包括：风险管理、取证、防火墙、入侵检测系统、Windows安全、LINIX／Anux安全、万维网、电子邮件、服务器应用、域名系统、安全通信、安全评估、安全评价和安全测试等。
本书由曹继军和林龙信翻译完成。
李化负责审校和统稿。
在翻译本书的过程中，我们仔细地推敲了相关的术语，并重点参阅了常用的翻译方法，但是在日常交流时，我们常常使用某些英文术语而不是其中文翻译，因此我们推荐读者更多地关注英文术语及其缩写。

<<网络安全宝典>>

内容概要

●理解当前的威胁和攻击以及它们是如何奏效的　　● 回答30个关键问题并了解当前的网络安全态势　　● 考虑任务适应性并确保关键功能正常运行　　● 精通密码术、隐写术、VPN以及其他隐蔽通信　　● 掌握确保Windows、Linux、浏览器、电子邮件以及无线网络等安全的有效方法　　● 探讨数字取证的基本要素，包括证据保全　　● 进行风险分析、制定全局计划，并为业务连续性和业务恢复做准备

作者简介

作者：（美国）科尔（Eric Cole） 译者：曹继军 林龙信 注释 解说词：李化

<<网络安全宝典>>

书籍目录

章节摘录

插图：（3）安装干净版本的操作系统，然后记录变更并生成ghost镜像。
（4）删除某些不必要的服务，然后记录变更并另外生成ghost镜像。
（5）如果固化过程中系统变得不可用，那么回退到最近的ghost镜像并再试一次。
然而，这时并不要删除在第（4）步骤中删除后会导致问题的服务。
（6）删除所有与操作系统同时加载的额外应用程序，然后记录变更并另外生成ghost镜像。
（7）检查并关闭工作站在执行任务时并非明确需要的所有端口。
检测已打开的端口的方法是打开Windows命令提示符窗口并运行netstat-ano命令，那么列出的状态为“LISTENING”的所有协议有已打开的端口。
（8）定位并关闭所有工作站发挥作用时并非明确需要的所有共享。
检测共享的方法是打开Windows命令提示符窗口并运行netshare命令，将列出所有共享的共享名和资源（文件夹）。
在Windows浏览器中单击文件夹的属性可以禁用共享。
（9）只安装必要的应用程序，记录变更并生成最终的ghost镜像。
（10）在Windows工作站安装个人防火墙。
（11）彻底测试该系统。
记录下系统固化过程中的每个步骤（无论成功或失败）非常重要。
如果失败，即通常为系统崩溃或死机，那么清楚知道已经执行了哪些步骤以便改变步骤是很重要的。
通常，失败是由禁用或删除了必要的服务引起的。
记录下成功固化系统的案例也非常重要。
为特定机构或用户固化系统的详细步骤描述对于未来增加系统很有价值。
通过Web搜索，可以获得大量固化各种Windows操作系统的步骤。
许多学院和大学最初为学生提供系统固化信息，并这些信息向公众发布。
现在，读者应该知道频繁产生ghost镜像的意义了。
产生ghost镜像的时间远小于第一次系统崩溃时重建系统所需的时间。
生成镜像的应用程序会为硬盘分区产生压缩的快照，该快照或镜像可以写入CDRW盘或存储在另外的硬盘分区中。
当系统固化后，彻底测试该系统非常重要。
微软很可能并没有测试您最终配置的系统。
实际上，个人所需要的服务和应用组合可能是唯一的。
使用net命令可以得到Windows服务列表。

版权说明