<<雷神的微软平台安全宝典>>

图书基本信息

书名：<<雷神的微软平台安全宝典>>

13位ISBN编号：9787302307433

10位ISBN编号：7302307431

出版时间：2013-1

出版时间：清华大学出版社

作者：(美)马伦(Mullen, T.) 著

译者：王晓华

<<雷神的微软平台安全宝典>>

内容概要

以最有效、最便捷的方式构建安全防护的基础设施
《雷神的微软平台安全宝典》为读者学习微软平台相关的安全技术提供了“一站式”解决方案，这些技术可以用于部署一些典型的基础安全设施。
本书从多个层面详细描述了安全相关的概念和方法论，包括服务器、客户端、组织结构、特定平台相关的安全选项、应用程序相关的安全特性(IIS、SQL、活动目录等)，还包括一些新的、从来没有发布过的安全工具，这些安全工具都带有完整的源代码。

主要内容
● 针对所有主流的微软应用程序的安全过程提供了详实的技术信息
● 采用独特的、基于项目的“讲故事”表达方式，同时组合多种安全技术和方法以应对现实世界中实际商业模式面临的安全挑战
● 内容的组织方式使得访问特定应用程序的安全技术和方法变得易如反掌
● 采用独特的观点和视角，使读者对解决特定应用程序安全方案的方法不仅“知其然”，而且“知其所以然”
● 随书发布的DVD光盘包含了源代码、工具、视频教程以及其他有用的资料

<<雷神的微软平台安全宝典>>

作者简介

作者：（美国）马伦（Timothy Mullen） 译者：王晓华 马伦（Timothy Mullen），是某个价值数十亿美元的商务平台的首席安全架构师，该商务平台在全球范围内被广泛应用。
Timothy被称为“雷神”，也是“上帝之锤”安全合作组织的创始人。
他是美国门萨俱乐部的成员、微软的认证讲师。
对于微软新发布的每一款操作系统，他都通过了微软工程师认证，在Windows企业安全领域连续4年被授予MVP称号。

<<雷神的微软平台安全宝典>>

书籍目录

章节摘录

版权页： 插图： 下面列出了几种能够立即解决这个问题以及与之相关的其他问题的方法：1）可以保持DefaultAppPool配置不变，而将虚拟目录显式地配置成指定的用户账户只能访问指定的资源这种方式，这样就可以不使用应用程序池的上下文。
换句话说，可以将用户直接指派给虚拟目录的管道，这个用户将被赋予访问用户共享目录的权限。
当然还有更简单的方法，那就是直接把用户添加到gShared全局组中。
这样做产生的问题也是显而易见的，必须将目录访问设置成用户的上下文（身份）。
通过虚拟目录访问文件就像用户直接访问文件一样。
因为既然用户已经必然地拥有了访问目录结构的权限，当然也就不需要再显式地对资源访问请求进行认证了。
2）可以修改DefaultAppPool配置，让应用程序池显式地使用某个用户的上下文。
正如前面提到的，这样做有相同的用户限制，但是虚拟目录可以使用应用程序池的上下文，不用像第一种方法那样必须指定某个用户。
这样就允许用户通过应用程序池建立的管道通过认证，当然用户还是需要登录以便能够访问管道（基于NTFS权限）。
但是，修改DefaultAppPool配置可能会导致那些正在使用DefaultAppPool的应用程序出现问题，不过是否出现问题最终还是取决于你的环境（系统）。
3）可以创建新的应用程序池并让这个应用程序池在指定用户账户的上下文环境中运行。
除了不使用默认的应用程序池以外，这种方法实现起来和第二种方法很类似。
这是目前最好的方法，定制的新应用程序池与其他应用程序池和进程完全隔离，可以对这个应用程序池做任何操作，这些操作都不会影响到其他应用程序。
还可以将用户账户限定为只能在此应用程序池的应用程序中使用。
你现在应该已经猜到了吧，我们将会采用第三种解决方法，因为使用这种方法可以给配置和管理带来极大的灵活性。
现在要做的事情就是确定使用哪种类型的用户账户，我喜欢将之作为服务账户来引用，因为这个账户是要指派给进程而不是某个用户的。
当然想怎么做都可以，不一定要和我一样。
我还喜欢给服务账户限定访问范围，这样就可以严格地控制当服务用户上下文中因执行能力（权限）不足而发生违约事件时，服务账户能够接触到哪些东西。
这其实是最小特权的概念，只赋予进程完成功能所需的最低权限，一点也不多给。
让进程在高特权的上下文中执行是危险的，进程可以利用这些特权做它们正常情况下不能做的事情，比如添加用户、创建文件或访问一些有重要价值的组。

<<雷神的微软平台安全宝典>>

编辑推荐

《雷神的微软平台安全宝典》从多个层面详细描述了安全相关的概念和方法论，包括服务器、客户端、组织结构、特定平台相关的安全选项、应用程序相关的安全特性（IIS、SQL、活动目录等），还包括一些新的、从来没有发布过的安全工具，这些安全工具都带有完整的源代码。

<<雷神的微软平台安全宝典>>

版权说明