□□服务器加固:加固基于windows2003平台的WEB服务器

□□

基于Windows平台下IIS运行的网站总给人一种感觉就是脆弱。早期的IIS确实存在很多问题，不过我个人认为自从Windows Server 2003发布后，IIS6及Windows Server 2003新的安全特性、更加完善的管理功能和系统的稳定性都有很大的增强。虽然从Windows Server 2003上可以看到微软不准备再发展ASP，特别是不再对Access数据库的完好支持，但是面对它的那些优势迫使我不得不舍弃Windows 2000 Server。况且我也不需要运行太多的ASP+Access，因为我的程序都是PHP+MySQL(说实话我不喜欢微软的ASP和ASPNET)，而且我确实信赖Windows Server 2003!

□□

服务器、网站，看到这些词大家都会想到什么，不只是性能更加关注的是它的安全问题。很多人都无法做到非常完美的安全加固，因为大部分的资料都来源互联网，而互联网的资料总不是那么详尽，毕竟每个服务器的应用环境及运行程序不同。

□□

我从事互联网这个行业只有2年时间，其间遇到了很多问题，我所管理的服务器部分是开放式(PUBLIC)的，它是向互联网的用户敞开的，所以我所面临的问题就更加的多!安全性首当其要，其次是系统的稳定性，最后才是性能。要知道服务器上存在很多格式各样的应用程序，有些程序本身就有缺陷，轻者造成服务器当机，严重的会危及到服务器的整个数据安全。

□□举个例子，有一台运行着300多个网站的Windows 2000 Server，一段时间里它经常Down机，发现内存泄漏特别快，几分钟时间内存使用立刻飙升到900M甚至高达1.2G，这个时候通过远程是无法访问服务器了，但是服务器系统本身却还在运行着。这个问题着实让我头疼了很长一段时间，因为如果要排查故障就要从这些网站入手，而网站的数量阻碍了我的解决进度。后来通过Filemon监控文件读取来缩小排查范围，之后对可疑网站进行隔离，最终找到故障点并解决。要知道一段小小的代码就可以让运行IIS5的Windows 2000 Server 挂掉!而在Windows Server 2003下，应用程序的级别低中高级变更为了程序池，这样我们就可以对一个池进行设置对内存和CPU进行保护。它的这一特性让我减轻了很多的工作量并且系统也稳定了很多。

□□

另外严重的就是安全性的问题了，无论任何文章都有一个宗旨就是尽量在服务器少开放端口，并开放必要的服务，禁止安装与服务器无关的应用程序。在 Windows 2000 Server中，目录权限都是Everyone，很多服务都是以SYSTEM权限来运行的，如Serv-U FTP这款出色的FTP服务器平台曾经害苦了不少人，它的溢出漏洞可以使入侵者轻松的获取系统完全控制权，如果做到呢?就是因为Serv-U FTP服务使用SYSTEM权限来运行，SYSTEM的权利比Administrator的权利可大的多，注册表SAM项它是可以直接访问和修改的，这样入侵者便利用这一特性轻松在注册表中克隆一个超级管理员账号并获取对系统的完全控制权限。

□□我的目标:加固WEB服务器系统，使之提高并完善其稳定性及安全性。

□□系统环境:Windows Server 2003 Enterprise Edition With Service Pack 1(以下简称W2k3SP1), WEB平台为IIS6, FTP平台为Serv-U FTP Server

□□安装配置操作系统

□□

安装操作系统, 在安装前先要先去调整服务器的BIOS设置, 关闭不需要的I/O, 这样节省资源又可以避免一些硬件驱动问题。务必断开服务器与网络的连接, 在系统没有完成安全配置前不要将它接入网络。在安装过程中如果网卡是PNP类型的, 那么应当为其网络属性只配置允许使用TCP/IP协议, 并关闭在
TCP/IP上的NETBIOS, 为了提供更安全的保证, 应该启用TCP/IP筛选, 并不开放任何TCP端口。完成操作系统的安装后, 首次启动
W2K3SP1, 会弹出安全警告界面, 主要是让你立刻在线升级系统更新补丁, 并配置自动更新功能, 这个人性化的功能是W2K3SP1所独有的, 在没有关闭这个警告窗口前, 系统是一个安全运行的状态, 这时我们应当尽快完成系统的在线更新。

□□

修改Administrator和Guest这两个账号的密码使其口令变的复杂, 并通过组策略工具为这两个敏感账号更名。修改位置在组策略中Computer Configuration-Windows Settings-Security Setting-Local Policies-Security
Options下, 这样做可以避免入侵者马上发动对此账号的密码穷举攻击。

□□服务器通常都是通过远程进行管理的, 所以我使用系统自带的组件
“远程桌面”来对系统进行远程管理。之所以选择它, 因为它是系统自带的组件缺省安装只需要去启用它就可以使用, 支持驱动器映射、剪切板映射等应用, 并且只要客户端是WindowsXP
PRO都会自带连接组件非常方便, 最主要还有一点它是免费的。当然第三方优秀的软件也有如:PCAnyWhere, 使用它可以解决Remote
Desktop无法在本地环境模式下工作的缺点。为了防止入侵者轻易地发现此服务并使用穷举攻击手段, 可以修改远程桌面的监听端口:

□□HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\WinStations\connection

□□注意:上面的注册表项是一个路径;它已换行以便于阅读。

□□3. 找到“PortNumber”子项, 您会看到值 00000D3D, 它是 3389
的十六进制表示形式。使用十六进制数值修改此端口号, 并保存新值。

□□注意:由于在终端服务器 4.0
版中尚未完全实现备用端口功能, 因此只是“在合理的限度内尽量”提供支持, 如果出现任何问题, Microsoft 可能要求您将端口重设为 3389。

□□

原文来源:微软知识库KB187623。当然为了达到更加安全的访问，还可以采用IPSec来保护远程桌面的连接访问。

□□

禁用不必要的服务不但可以降低服务器的资源占用减轻负担，而且可以增强安全性。下面列出了可以禁用的服务:

□□Application Experience Lookup Service

□□Automatic Updates

□□1. 运行 Regedt32 并转到此项:

□□HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp

□□注意:上面的注册表项是一个路径;它已换行以便于阅读。

□□2. 找到“PortNumber”子项，您会看到值 00000D3D，它是 3389 的十六进制表示形式。使用十六进制数值修改此端口号，并保存新值。

□□要更改终端服务器上某个特定连接的端口，请按照下列步骤操作: 运行 Regedt32 并转到此项:

□□BITS

□□Computer Browser

□□DHCP Client

□□Error Reporting Service

□□Help and Support

□□Network Location Awareness

□□Print Spooler

□□Remote Registry

□□Secondary Logon

□□Server

□□Smartcard