WIN2000SERVER安全配置技巧58条（一） PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/140/2021_2022_WIN2000SER_c100_140027.htm WIN2000 SERVER是比较流行的服务器操作系统之一，但是要想安全的配置微软的这个操作系统，却不是一件容易的事。本文搜集整理了58条针对WIN2000 SERVER进行安全配置的注意事项或技巧。 1.NTFS比FAT分区多了安全控制功能，可以对不同的文件夹设置不同的访问权限，安全性增强。 2.建议最好一次性全部安装成NTFS分区，而不要先安装成FAT分区再转化为NTFS分区，这样做在安装了SP5和SP6的情况下会导致转化不成功，甚至系统崩溃。 3.安装NTFS分区有一个潜在的危险，就是目前大多数反病毒软件没有提供对软盘启动后NTFS分区病毒的查杀，这样一旦系统中了恶性病毒而导致系统不能正常启动，后果就比较严重，因此及建议平时做好防病毒工作。 4.分区和逻辑盘的分配：推荐的安全配置是建立三个逻辑驱动器，第一个大于2G，用来装系统和重要的日志文件，第二个放IIS，第三个放FTP，这样无论IIS或FTP出了安全漏洞都不会直接影响到系统目录和系统文件。要知道，IIS和FTP是对外服务的，比较容易出问题。而把IIS和FTP分开主要是为了防止入侵者上传程序并从IIS中运行。 5.安装顺序的选择：win2000在安装中有几个顺序是一定要注意的。 首先，何时接入网络，Win2000在安装时有一个漏洞，在你输入Administrator密码后，系统就建立了ADMIN$的共享，但是并没有用你刚刚输入的密码来保护它，这种情况一直持续到你再次启动后，在此期间，任何人都可以通过ADMIN$进入你的机器；同时，只要安装一完成

，各种服务就会自动运行，而这时的服务器是满身漏洞，非常容易进入的，因此，在完全安装并配置好win2000 SERVER之前，一定不要把主机接入网络。 其次，补丁的安装：补丁的安装应该在所有应用程序安装完之后，因为补丁程序往往要替换/修改某些系统文件，如果先安装补丁再安装应用程序有可能导致补丁不能起到应有的效果，例如：IIS的HotFix就要求每次更改IIS的配置都需要安装。 6.端口是计算机和外部网络相连的逻辑接口，也是计算机的第一道屏障，端口配置正确与否直接影响到主机的安全，一般来说，仅打开你需要使用的端口会比较安全，配置的方法是在网卡属性-TCP/IP-高级-选项-TCP/IP筛选中启用TCP/IP筛选，不过对于win2000的端口过滤来说，有一个不好的特性：只能规定开哪些端口，不能规定关闭哪些端口，这样对于需要开大量端口的用户就比较痛苦。 7.IIS是微软的组件中漏洞最多的一个，平均两三个月就要出一个漏洞，而微软的IIS默认安装又实在不敢恭维，所以IIS的配置是我们的重点，现在大家跟着我一起来：首先，把C盘那个什么Inetpub目录彻底删掉，在D盘建一个Inetpub（要是你不放心用默认目录名也可以改一个名字，但是自己要记得）在IIS管理器中将主目录指向D:\Inetpub；其次，那个IIS安装时默认的什么scripts等虚拟目录一概删除，如果你需要什么权限的目录可以自己慢慢建，需要什么权限开什么。（特别注意写权限和执行程序的权限，没有绝对的必要千万不要给）第三，应用程序配置：在IIS管理器中删除必须之外的任何无用映射，必须指的是ASP，ASA和其他你确实需要用到的文件类型，例如你用到stml等（使用server side include），实际上90%的主机有了上面两个映射就够了，其余

的映射几乎每个都有一个凄惨的故事：htw，htr，idq，ida……想知道这些故事？去查以前的漏洞列表吧。在IIS管理器中右击主机->属性->WWW服务 编辑->主目录配置->应用程序映射，然后就开始一个个删吧（里面没有全选的）。接着在刚刚那个窗口的应用程序调试书签内将脚本错误消息改为发送文本（除非你想ASP出错的时候用户知道你的程序/网络/数据库结构）错误文本写什么？随便你喜欢，自己看着办。点击确定退出时别忘了让虚拟站点继承你设定的属性。安装新的Service Pack后，IIS的应用程序映射应重新设置。（说明：安装新的Service Pack后，某些应用程序映射又会出现，导致出现安全漏洞。这是管理员较易忽视的一点。） 为了对付日益增多的cgi漏洞扫描器，还有一个小技巧可以参考，在IIS中将HTTP404 Object Not Found出错页面通过URL重定向到一个定制HTM文件，可以让目前绝大多数CGI漏洞扫描器失灵。其实原因很简单，大多数CGI扫描器在编写时为了方便，都是通过查看返回页面的HTTP代码来判断漏洞是否存在的，例如，著名的IDQ漏洞一般都是通过取1.idq来检验，如果返回HTTP200，就认为是有这个漏洞，反之如果返回HTTP404就认为没有，如果你通过URL将HTTP404出错信息重定向到HTTP404.htm文件，那么所有的扫描无论存不存在漏洞都会返回HTTP200，90%的CGI扫描器会认为你什么漏洞都有，结果反而掩盖了你真正的漏洞，让入侵者茫然无处下手，不过从个人角度来说，我还是认为扎扎实实做好安全设置比这样的小技巧重要的多。 最后，为了保险起见，你可以使用IIS的备份功能，将刚刚的设定全部备份下来，这样就可以随时恢复IIS的安全配置。还有，如果你怕IIS负荷过高导致服务器

满负荷死机，也可以在性能中打开CPU限制，例如将IIS的最大CPU使用率限制在70%。 8.帐号尽可能少，且尽可能少用来登录 说明：网站帐号一般只用来做系统维护，多余的帐号一个也不要，因为多一个帐号就会多一份被攻破的危险。 a.除Administrator外，有必要再增加一个属于管理员组的帐号；说明：两个管理员组的帐号，一方面防止管理员一旦忘记一个帐号的口令还有一个备用帐号；另方面，一旦黑客攻破一个帐号并更改口令，我们还有有机会重新在短期内取得控制权。 b.所有帐号权限需严格控制，轻易不要给帐号以特殊权限；将Administrator重命名，改为一个不易猜的名字。其他一般帐号也应尊循这一原则； 说明：这样可以为黑客攻击增加一层障碍。 c.将Guest帐号禁用，同时重命名为一个复杂的名字，增加口令，并将它从Guest组删掉； 说明：有的黑客工具正是利用了guest 的弱点，可以将帐号从一般用户提升到管理员组。 d.给所有用户帐号一个复杂的口令（系统帐号出外），长度最少在8位以上， 且必须同时包含字母、数字、特殊字符。同时不要使用大家熟悉的单词（如microsoft）、熟悉的键盘顺序（如qwert）、熟悉的数字（如2000）等； 说明：口令是黑客攻击的重点，口令一旦被突破也就无任何系统安全可言了，而这往往是不少网管所忽视的地方，据我们的测试，仅字母加数字的5位口令在几分钟内就会被攻破，而所推荐的方案则要安全的多。 e.口令必须定期更改（建议至少两周该一次），且最好记在心里，除此以外不要在任何地方做记录；另外，如果在日志审核中发现某个帐号被连续尝试，则必须立刻更改此帐号（包括用户名和口令）； 说明：在帐号属性中设立锁定次数，比如改帐号失败登录次数超过5次即

锁定改帐号。这样可以防止某些大规模的登录尝试，同时也使管理员对该帐号提高警惕。