文章编号：1006-4354 (2003) 01-0039-05

WIN2000 服务器的安全设置和防范措施

赵世发[1]，王治平[1]，石明生[2]，刘　波[3]，瑚成英[1]，刘　磊[1]
(1. 商洛市气象局，陕西商洛　726000；2. 安康市气象局，陕西安康　725000；
3. 陕西省防雷中心，陕西西安　710014)

中图分类号：TP393.0　　文献标识码：B

目前，WIN2000 SERVER 是比较流行的服务器操作系统之一，而微软的产品是以 Bug &Patch 而著称的，中文版的 Bug 远远多于英文版，它的安全漏洞比较多，本文试图对 WIN2000 SERVER 的安全配置和安全漏洞进行较详细的分析探讨，并结合互联网上最新的黑客攻击手段以及多个网管员的经验，提出一些有效的防范措施。

1　正确安装 WIN2000 SERVER

1.1　安装准备工作

IIS、FTP 或数据库是对外服务的，会有泄漏源码/溢出的漏洞，如果把系统和它们放在同一个驱动器上，会导致系统文件的泄漏，甚至入侵者远程获取 ADMIN $。推荐的安全配置是建立 5 个逻辑分区，第 1 个分区用来装系统和重要的日志文件，大小为 2～3GB，第 2 个放 IIS，第 3 个放 FTP，第 4 个安装数据库，第 5 个做备份，这样无论 IIS、FTP 或数据库出了安全漏洞都不会直接影响到系统目录和系统文件。

硬盘分区均为 NTFS 分区，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。最好一次全部

收稿日期：2002-09-23

作者简介：赵世发 (1966-)，男，陕西商南人，工程师，从事预报、通信工作。

120 dgpm 的机率为 21/28；如较强应≥190 dgpm，则易发生春夏连旱，机率为 4/5。副高面积指数≤8 dgpm 的机率为 20/28。若面积指数偏大≥140 dgpm，易发生春夏连旱，其机率为 3/4。

4.4　冬季降水量

冬季 (12—2 月) 的降水量为正常或偏多，即 R≥18.0 mm，发生春旱的机率为 17/28。而前 1 a 12 月降水量偏少，R≤3.1 mm 时的机率为 18/28。当年 1 月份降水量偏多，R≥6.0 mm 时的机率为 15/28。

5　小结

5.1　干旱空间分布不均匀，川塬多于山区，海拔高度低的地方发生干旱的频率较高，扶风和眉县的干旱发生率最高，太白最少。

5.2　时间分布上具有明显的季节性和持续性，年变化具有周期性。月变化呈现波动形式。发生春旱和春夏连旱的频率较高，局部干旱持续时间最长可达 5 个月，区域性干旱持续时间最长可达 4 个月。60、80 年代干旱较少，70、90 年代干旱较多，年代际变化有准 20 a 的振荡周期。

5.3　几乎每年都有小旱发生，大旱发生率为 12%，中旱发生率为 27%。历史上干旱最严重的年份是 1979 年，春旱最严重的是 2000 年。

5.4　春旱发生与 1 月份的环流特征量有较好的对应关系，1 月极涡偏西、偏东、偏北，副高西伸脊点偏东、强度偏弱，宝鸡易发生春旱。

5.5　前期冬季降水量偏多；前 1 a 12 月降水量偏少；1 月份降水量偏多，宝鸡易发生春旱。

参考文献：

[1]　吕从中．陕西省农业气候区划 [M]．西安：西安地图出版社，1988.

安装成 NTFS 分区，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软盘启动后对 NTFS 分区病毒的查杀，这样一旦系统中了恶性病毒而不能正常启动，后果就比较严重，因此应平时做好防病毒工作（在线监控）。

安装成独立的域控制器，选择工作组成员，不选择域。

1.2 定制自己所需的 WIN2000 SERVER

以 WIN2000 简体中文版为例，WIN2000 在默认情况下会安装一些常用的组件，这个默认安装是极度危险的（很容易进入任何一台默认安装的服务器），应该确切的知道需要哪些服务，根据最少的服务＋最小的权限＝最大的安全原则，仅安装确实需要的服务。典型的 WEB 服务器需要的最小组件选择是：只安装 IIS 的 Com Files，IIS Snap-In，WWW Server 组件。如果确实需要安装其他组件，需慎重，特别是：Indexing Service，FrontPage 2000 Server Extensions，Internet Service Manager（HTML）这几个危险服务。

1.3 管理应用程序的选择

选择一个好的远程管理软件是非常重要的，这不仅仅是安全方面的要求，也是应用方面的需要。WIN2000 的 Terminal Service 是基于 RDP（远程桌面协议）的远程控制软件，他的速度快，操作方便，比较适合用来进行常规操作。但是，Terminal Service 也有其不足之处，为了安全起见，最好再配备一个远程控制软件作为辅助，和 Terminal Service 互补，像 PcAnyWhere。

1.4 安装顺序的选择

WIN2000 在安装时有一个漏洞，输入 Administrator 密码后，系统就建立了 ADMIN $ 的共享，但是并没有用刚刚输入的密码来保护它，这种情况一直持续到再次启动后，在此期间，任何人都可以通过 ADMIN $ 进入系统；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，因此，在完全安装并配置好 WIN2000 SERVER 之前，不要把主机接入网络。

补丁的安装应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无效，例如：IIS 的 HotFix 就要求每次更改 IIS 的配置后都需要重新安装补丁。

1.5 及时安装补丁程序

补丁程序是微软公司针对软件出现的安全漏洞进行修补的程序，每几个月就有 1 个补丁包发布，所以，要及时安装补丁程序系统才会安全。2002 年 8 月发布了 SP3 补丁包，在此之前需要更新的补丁程序有 14 个，SP3 集成了 SP1、SP2 等多个补丁程序，现在全部更新的补丁程序如下（有 6 个）：

Windows 2000 Hotfix （Pre-SP4） [See Q320206 for more information]

Windows 2000 Hotfix （Pre-SP4） [See Q321599 for more information]

Windows 2000 Hotfix （Pre-SP4） [See Q322842 for more information]

Windows 2000 Hotfix （Pre-SP4） [See Q326830 for more information]

Windows 2000 Hotfix （Pre-SP4） [See Q326886 for more information]

Windows 2000 Service Pack 3

2 安全配置 WIN2000 SERVER

即使正确安装了 WIN2000 SERVER，系统还是有很多的漏洞，需进一步进行细致地配置。

2.1 端口、协议和服务的安全配置

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，仅打开需要使用的端口是比较安全的，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，WIN2000 的端口过滤：只能开端口，不能关闭端口，为此，微软推出了 IIS 功能锁定程序 IIS Lockdown Wizard 2.1 版。应用这一软件，可以在向导的帮助下对系统中不用的功能和端口进行关闭，为系统提供多层保护。

2.1.1 只开放必要的端口其余关闭 缺省情况下，所有的端口对外开放，黑客就会利用扫描工具扫描这些端口，找到可以利用的端口，进行攻击。一些常用端口列表如下：

端口	协议	应用程序
21	TCP	FTP
25	TCP	POP3
53	TCP	DNS
80	TCP	HTTP SERVER
110	TCP	SMTP
1433	TCP	SQL SERVER
5631	TCP	PCANYWHERE
5632	UDP	PCANYWHERE

根据需要开放，暂时不用的就关闭。

2.1.2　只保留 TCP/IP 协议，删除 NETBEUI、IPX/SPX 协议　网站需要的通讯协议只有 TCP/IP，而 NETBEUI 和 IPX/SPX 是用于局域网的协议，一般不用，如不删除反而会被某些黑客工具利用。

2.1.3　只保留与网站有关的服务和服务器某些必须的服务　有些服务如 RAS 服务、Spooler 服务等会给黑客带来可乘之机，如果确实没有用，建议禁止掉，但要注意有些服务是操作系统必须的服务，建议在停掉前查阅帮助文档并首先在测试服务器上作一下测试。

2.1.4　加强日志记录和审核　日志包括事件查看器中的应用、系统、安全日志，IIS 中的 WWW、SMTP、FTP 日志、SQL SERVER 日志等，从中可以看出某些攻击迹象，因此查看日志是保证系统安全必不可少的环节。安全日志缺省是不记录，要自己选上，但只需选取真正关心的指标就可以了，如果全选，则记录数目太大，反而不利于分析。

2.2　IIS 安全配置

IIS 是微软的组件中漏洞最多的，平均两三个月就要出一个漏洞，而微软的 IIS 默认安装又存在很多安全漏洞，所以 IIS 的配置是重点。

2.2.1　只安装必须的服务　建议只安装必须的服务，如 WWW 服务、FTP 服务不要安装 Index Server、FrontPage Server Extensions 功能。

2.2.2　删除默认安装的 Inetpub 目录和不必要的 IIS 扩展名映射　把 C 盘默认安装的 Inetpub 目录删掉，在 D 盘建一个 WEB（不用默认目录名而改一个名字）在 IIS 管理器中将主目录指向 D:\WEB，IIS 安装时默认的 Scripts 等虚拟目录也一概删除（减少安全漏洞），需要什么权限的目录可以自己再建，需要什么权限再开。

在 IIS 管理器中删除不必要的 IIS 扩展名映射。最好去掉 .IDC、.HTR、.STM、.IDA、.HTW 应用程序映射，.shtml、.shtm 等如果无用，也应去掉，实际上 90%的主机有了（ASP、ASA、HTM）3 个映射就够了，其余的映射几乎都有安全隐患。注意，让虚拟站点继承上述设定的属性。

2.2.3　出错页面通过 URL 重定向到一个定制 HTM 文件　为了对付日益增多的 CGI 漏洞扫描器，在 IIS 中将 HTTP404 Object Not Found 出错页面通过 URL 重定向到一个定制的 HTTP404.htm 文件，可以让目前绝大多数 CGI 漏洞扫描器失灵。

2.2.4　安装新的 Service Pack 后，IIS 的应用程序映射应重新设置　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。

2.2.5　设置 IP 拒绝访问列表　对于 WWW 服务，可以拒绝一些对站点有攻击嫌疑的地址；尤其对于 FTP 服务，如果只是自己公司和特定用户上传文件，就可以只允许本公司和特定用户的 IP 访问 FTP 服务器。

2.2.6　禁止对 FTP 服务的匿名访问　如果允许对 FTP 服务做匿名访问，该匿名账户就有可能被利用来获取更多的信息，对系统造成危害。

2.2.7　建议慎重设置 WEB 站点目录的访问权限，使用 W3C 扩充日志文件格式　不要给予目录以写入和允许目录浏览权限。只给予 .ASP 文件目录以脚本的权限，而不要给执行权限。每天记录客户 IP 地址，用户名，服务器端口，方法，URI 字根，HTTP 状态，用户代理，而且要定期审查日志。最好不要使用缺省的目录，建议更换一个记日志的路径，同时设置日志的访问权限，只允许管理员和 system，这样既可以发现攻击的迹象，采取预防措施，也可以作为受攻击的一个证据。

2.2.8　用 IIS 功能锁定程序 IIS Lockdown Wizard 2.1 版 锁定不需要的功能、服务。

2.2.9 备份 IIS 的安全配置 为了保险起见，使用 IIS 的备份功能，将上述的设定全部备份下来，这样就可以随时恢复 IIS 的安全配置。

2.3 账号安全

WIN2000 的默认安装是允许任何用户通过空用户得到系统所有账号/共享列表，这本来是为了方便局域网用户共享文件的，但是远程用户也可以得到系统的用户列表并使用暴力法破解用户密码，应采用以下账号策略。

2.3.1 账号尽可能少 因为多一个账号就会多一份被攻破的危险。

2.3.2 改 Administrator 账号名，并再增加一个属于管理员组的备用账号；一旦黑客攻破一个账号并更改口令，还有机会重新取得控制权。

2.3.3 所有账号权限需严格控制，轻易不要给账号以特殊权限。

2.3.4 将 Gues 账号禁用，同时重命名一个复杂的名字，增加口令，并将它从 Guest 组删掉。

2.3.5 给所有用户账号一个复杂的口令，口令必须定期更改，在账号属性中设立锁定次数。

2.3.6 更改注册表参数 更改注册表参数 Local _ Machine\System\CurrentControlSet\Control\LSA-RestrictAnonymous = 1 来禁止 139 空连接，更改注册表参数 HKEY _ LOCAL _ MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\winlogon 项中的 Don't Display Last User Name 串数据改成 1，这样系统不会自动显示上次的登录用户名。

2.3.7 改 NTFS 的安全权限 NTFS 下所有文件默认情况下对所有人（EveryOne）为完全控制权限，这使黑客有可能使用一般用户身份对文件做增加、删除、执行等操作，建议改为读取权限，而只给管理员和 System 以完全控制权限。

2.3.8 备份注册表 为了保险起见，使用注册表导出功能，将设定好的注册表备份下来，这样一旦注册表有问题就可以随时导入正确的注册表。

2.4 加强网站各种数据备份

站点的核心是数据，数据一旦遭到破坏后果不堪设想，而这往往是黑客们真正关心的东西；数据备份需要仔细计划，制定出一个策略并进行测试以后再实施，而且随着网站的更新，备份计划也需要不断地调整。

2.5 用最新的安全漏洞扫描软件扫描服务器，并根据扫描结果进行改进。

3 ASP 编程对 WIN2000 服务器造成的安全漏洞

安全不仅是网管员的事，编程人员也必须在某些安全细节上注意。涉及用户名与口令的程序最好封装在服务器端，尽量少的在 ASP 文件里出现，涉及到与数据库连接的用户名与口令应给予最小的权限。一些文件泄露问题应按以下方法处理。

3.1 防止 ASP 主页 .inc 文件泄露问题

解决方案：首先对 .inc 文件内容进行加密，其次也可以使用 .asp 文件代替 .inc 文件使用户无法从浏览器直接观看文件的源代码；.inc 文件的文件名不用系统默认的或者有特殊含义的或容易被用户猜测到的，尽量使用无规则的英文字母。

在处理类似留言板、BBS 等输入框的 ASP 程序中，最好屏蔽掉 HTML、JavaScript、VBScript 语句。如无特殊要求，可以限定只允许输入字母与数字，屏蔽掉特殊字符，同时对输入字符的长度进行限制。而且要在客户端进行输入合法性检查，同时要在服务器端程序中进行类似检查。

3.2 防止 ACCESS mdb 数据库有可能被下载的漏洞

解决方法：第一 为数据库文件名称起个复杂的名字，并把他放在几层目录下。其次不要把数据库名直接写在程序中。第三是使用 ACCESS 来为数据库文件编码及加密。

4 SQL SERVER 的安全

SQL SERVER 是 WIN2000 平台上用的最多的数据库系统，但是它的安全问题也较突出。

4.1 及时更新补丁程序

与 WIN2000 一样，SQL SERVER 的许多漏洞会由补丁程序来弥补。建议在安装补丁程序之前先在测试机器上做测试，同时提前做好目标服务器的数据备份。

4.2 给 SA 一个复杂的口令

SA 具有对 SQL SERVER 数据库操作的全

部权限。

4.3 严格控制数据库用户的权限

轻易不要给用户对表有直接的查询、更改、插入、删除权限，可以通过给用户以访问视图的权限，以及只具有执行存储过程的权限。

5 PCANYWHERE 的安全

PCANYWHERE 是最流行的基于 NT 与 2000 的远程控制工具，同样也需要注意安全问题。建议采用单独的用户名与口令，采用加密手段。不要采用与 NT 管理员一样的用户名与口令，及时安装较新的版本。

6 系统的安全监控和定期维护

地、县级信息网站大部分没有专用防火墙，服务器安全没有保障，使用防毒（防黑客程序）在线监控并能清除软件是非常必要的。KV3000 杀毒王功能较多，占用内存少，安装使用简单是首选软件。KV3000 杀毒王新增邮件监视、邮箱病毒直接查杀，各种邮件病毒、黑客程序清除功能；还有恶意网页监视和实时清除、注册表监视并提示用户处理方法等功能。所以，应安装 KV3000 杀毒王对服务器进行在线安全监控。同时，也应定期用 KV3000 杀毒王、木马克星和其它的杀毒软件对服务器操作系统和网站数据进行全面查杀和系统性地维护。

7 WIN2000 服务器中木马通用解法和最新病毒、木马清除方法

虽然现在市面上有很多新版杀毒软件都可以自动清除“木马”，但它们并不能防范新出现的“木马”程序，因此还需要知道一些根据“木马”的启动原理而用的新的查杀方法。

在 WIN2000 系统中可能加载“木马”程序的地方有，在 win.ini 文件中的[WINDOWS]下面，“run＝”和“load＝”的地方，在 system.ini 文件中的 [BOOT] 下面有个“shell＝文件名”。正确的文件名应该是“explorer.exe”，如果不是“explorer.exe”，而是“shell＝ explorer.exe 程序名”，那么后面跟着的那个程序就是“木马”程序。在注册表中的情况最复杂，通过 regedit 命令打开注册表编辑器，在 HKEY－LOCAL－MACHINE\Software\Microsoft\Windows\CurrentVersion\Run”目录下，查看键值中有没有自己不熟悉的自动启动文件，扩展名为 EXE。如果有，可能是木马，知道了“木马”可能隐藏的地方，查杀“木马”就变得容易了，如果发现有“木马”存在，最安全也是最有效的方法就是马上将计算机与网络断开，防止黑客通过网络对系统进行攻击。然后编辑 win.ini 文件，将［WINDOWS］下面，“run＝‘木马’程序”或“load＝‘木马’程序”更改为“run＝”和“load＝”；编辑 system.ini 文件，将［BOOT］下面的“shell＝‘木马’文件”，更改为：“shell＝explorer.exe”；在注册表中，用 regedit 对注册表进行编辑，先在“HKEY－LOCAL－MACHINE\Software\Microsoft\Windows\CurrentVersion\Run”下找到“木马”程序的文件名，再在整个注册表中搜索并替换掉“木马”程序，有时候还需注意的是：有的“木马”程序并不是直接将“HKEY－LOCAL－MACHINE\Software\Microsoft\Windows\CurrentVersion\Run”下的“木马”键值删除就行了，因为有的“木马”如：BladeRunner“木马”，如果删除它，“木马”会立即自动加上，需要的是记下“木马”的名字与目录，然后退回到 MS－DOS 下，找到此“木马”文件并删除掉。重新启动计算机，然后再到注册表中将所有“木马”文件的键值删除。

查杀注册表病毒还有一种方法就是导入备份的注册表。

8 最新病毒、木马清除经验措施

建议定期到各大网站的病毒中心，查看最新发布的病毒、木马、后门程序代码，利用操作系统的搜索文件功能对系统进行全面搜索并删除，同时在注册表中也进行同样的搜索和删除。可以清除最新的病毒、木马、后门程序。