WIN2000SERVER安全配置技巧58条（二） 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_140020.htm 11.只安装一种操作系统； 说明：安装两种以上操作系统，会给黑客以可乘之机，利用攻击使系统重启到另外一个没有安全设置的操作系统（或者他熟悉的操作系统），进而进行破坏。 12.安装成独立的域控制器（Stand Alone），选择工作组成员，不选择域； 说明：主域控制器（PDC）是局域网中队多台联网机器管理的一种方式，用于网站服务器包含着安全隐患，使黑客有可能利用域方式的漏洞攻击站点服务器。 13.将操作系统文件所在分区与WEB数据包括其他应用程序所在的分区分开，并在安装时最好不要使用系统默认的目录，如将\WINNT改为其他目录； 说明：黑客有可能通过WEB站点的漏洞得到操作系统对操作系统某些程序的执行权限，从而造成更大的破坏。同时如果采用IIS的话你应该在其设置中删除掉所有的无用的映射，同时不要安装索引服务，远程站点管理与服务器扩展最好也不要要，然后删掉默认路径下的www，整个删，不要手软，然后再硬盘的另一个硬盘建立存放你网站的文件夹，同时一定记得打开w3c日志纪录，切记（不过本人建议采用apache 1.3.24） 系统安装过程中一定本着最小服务原则，无用的服务一概不选择，达到系统的最小安装，多一个服务，多一份风险，呵呵，所以无用组件千万不要安装！ 14.关于补丁，在NT下，如果安装了补丁程序，以后如果要从NT光盘上安装新的Windows程序，都要重新安装一次补丁程序，2000下不需要这样做。 说明：最新的补丁程序，表示系统以前有重大漏洞

，非补不可了，对于局域网内服务器可以不是最新的，但站点必须安装最新补丁，否则黑客可能会利用低版本补丁的漏洞对系统造成威胁。这是一部分管理员较易忽视的一点；安装NT的SP5、SP6有一个潜在威胁，就是一旦系统崩溃重装NT时，系统将不会认NTFS分区，原因是微软在这两个补丁中对NTFS做了改进。只能通过Windows 2000安装过程中认NTFS，这样会造成很多麻烦，建议同时做好数据备份工作。 安装Service Pack前应先在测试机器上安装一次，以防因为例外原因导致机器死机，同时做好数据备份。 尽量不安装与WEB站点服务无关的软件； 说明：其他应用软件有可能存在黑客熟知的安全漏洞。 15.解除NetBios与TCP/IP协议的绑定 说明：NetBois在局域网内是不可缺少的功能，在网站服务器上却成了黑客扫描工具的首选目标。方法：NT：控制面版网络绑定NetBios接口禁用 2000：控制面版网络和拨号连接本地网络属性TCP/IP属性高级WINS禁用TCP/IP上的NETBIOS。 16.删除所有的网络共享资源，在网络连接的设置中删除文件和打印共享，只留下TCP/IP协议 说明：2000在默认情况下有不少网络共享资源，在局域网内对网络管理和网络通讯有用，在网站服务器上同样是一个特大的安全隐患。（卸载“ Microsoft 网络的文件和打印机共享 ”。当查看“ 网络和拨号连接 ”中的任何连接属性时，将显示该选项。单击“ 卸载 ”按钮删除该组件；清除“ Microsoft 网络的文件和打印机共享 ”复选框将不起作用。） 方法： 1>2000：控制面版管理工具计算及管理共享文件夹停止共享 但上述方法太麻烦，服务器每重启一次，管理员就必须停止一次。 2>修改注册表：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

\LanmanServer\Parameters下增加一个键 Name: AutoShareServer Type: REG_DWORD value: 0 然后重新启动您的服务器，磁盘分区共享去掉，但IPC共享仍存在，需每次重启后手工删除。 17.改NTFS的安全权限； 说明：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，建议对一般用户只给予读取权限，而只给管理员和System以完全控制权限，但这样做有可能使某些正常的脚本程序不能执行，或者某些需要写的操作不能完成，这时需要对这些文件所在的文件夹权限进行更改，建议在做更改前先在测试机器上作测试，然后慎重更改。 18.加强数据备份； 说明：这一点非常重要，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；遗憾的是，不少网管在这一点上作的并不好，不是备份不完全，就是备份不及时。数据备份需要仔细计划，制定出一个策略并作了测试以后才实施，而且随着网站的更新，备份计划也需要不断地调整。 19.只保留TCP/IP协议，删除NETBEUI、IPX/SPX协议； 说明：网站需要的通讯协议只有TCP/IP，而NETBEUI是一个只能用于局域网的协议，IPX/SPX是面临淘汰的协议，放在网站上没有任何用处，反而会被某些黑客工具利用。 20.不要起用IP转发功能，控制面板->网络->协议->TCP/IP协议->属性，使这个选框为空。（NT） 说明：缺省情况下，NT的IP转发功能是禁止的，但注意不要启用，否则它会具有路由作用，被黑客利用来对其他服务器进行攻击。 