 由于Win2000操作系统良好的网络功能，因此在因特网中有部分网站服务器开始使用的Win2000作为主操作系统的。但由于该操作系统是一个多用户操作系统，黑客们为了在攻击中隐藏自己，往往会选择Win2000作为首先攻击的对象。那么，作为一名Win2000用户，我们该如何通过合理的方法来防范Win2000的安全呢?下面笔者搜集和整理了一些防范Win2000安全的几则措施，现在把它们贡献出来，恳请各位网友能不断补充和完善。 1、及时备份系统 为了防止系统在使用的过程中发生以外情况而难以正常运行，我们应该对Win2000完好的系统进行备份，最好是在一完成Win2000系统的安装任务后就对整个系统进行备份，以后可以根据这个备份来验证系统的完整性，这样就可以发现系统文件是否被非法修改过。如果发生系统文件已经被破坏的情况，也可以使用系统备份来恢复到正常的状态。备份信息时，我们可以把完好的系统信息备份在CD-ROM光盘上，以后可以定期将系统与光盘内容进行比较以验证系统的完整性是否遭到破坏。如果对安全级别的要求特别高，那么可以将光盘设置为可启动的并且将验证工作作为系统启动过程的一部分。这样只要可以通过光盘启动，就说明系统尚未被破坏过。 2、设置系统格式为NTFS 安装Win2000时，应选择自定义安装，仅选择个人或单位必需的系统组件和服务，取消不用的网络服务和协议，因为协议和服务安装越多，入侵者入侵的途径越多，潜在的系统安全隐患也越大。选

择Win2000文件系统时，应选择NTFS文件系统，充分利用NTFS文件系统的安全性。NTFS文件系统可以将每个用户允许读写的文件限制在磁盘目录下的任何一个文件夹内，而且Win2000新增的磁盘限额服务还可以控制每个用户允许使用的磁盘空间大小。 3、加密文件或文件夹 为了防别人偷看系统中的文件，我们可以利用Win2000系统提供的加密工具，来保护文件和文件夹。其具体操作步骤是，在“ Win 资源管理器 ”中，用鼠标右键单击想要加密的文件或文件夹，然后单击“ 属性 ”。单击“ 常规 ”选项卡上的“ 高级 ”，然后选定“ 加密内容以保证数据安全 ”复选框。 4、取消共享目录的EveryOne组 默认情况下，在Win2000中新增一个共享目录时，操作系统会自动将EveryOne这个用户组添加到权限模块当中，由于这个组的默认权限是完全控制，结果使得任何人都可以对共享目录进行读写。因此，在新建共享目录之后，要立刻删除EveryOne组或者将该组的权限调整为读取。 5、创建紧急修复盘 如果系统一不小心被破坏而不能正常启动时，就需要专用的Win2000系统启动盘，为此我们一定要记得在Win2000安装完好后创建一个紧急修复磁盘。在创建该启动盘时，我们可以利用Win2000的一个名为NTBACKUP.EXE的工具来实现。运行NTBACKUP.EXE，从工具栏中选择“ 创建紧急修复盘Create an Emergency Repair Disk ”在A：驱动器中插入一张空白格式化的软盘，并点击“ 确定 ”，点击“ 确定 ”到达完成信息，再点击“ 确定 ”。修复盘不再可以用来恢复用户帐号信息等，而且您必须备份/恢复Active Directory，在备份中将被覆盖。 6、改进登录服务器 将系统的登录服务器移到一个单独的机器中会增加系统的安全级别，使用一个

更安全的登录服务器来取代Win2000自身的登录工具也可以进一步提高安全。在大的Win2000网络中，最好使用一个单独的登录服务器用于登录服务。它必须是一个能够满足所有系统登录需求并且拥有足够的磁盘空间的服务器系统，在这个系统上应该没有其它的服务运行。更安全的登录服务器会大大削弱入侵者透过登录系统窜改日志文件的能力。 7、使用好安全机制 严格设计管理好Win2000系统的安全规则，其内容主要包括“ 密码规则 ”、“ 账号锁定规则 ”、“ 用户权限分配规则 ”、“ 审核规则 ” 以及“ IP 安全规则 ”。对全部用户都应按工作需要进行分组，合理对用户分组是进行系统安全设计的最重要的基础。利用安全规则可以限定用户口令的有效期、口令长度。设置登录多少次失败后锁定工作站，并对用户备份文件和目录、关机、网络访问等各项行为进行有效控制。 8、对系统进行跟踪记录 为了能密切地监视黑客的攻击活动，我们应该启动Win2000的日志文件，来记录系统的运行情况，当黑客在攻击系统时，它的蛛丝马迹都会被记录在日志文件中的，因此有许多黑客在开始攻击系统时，往往首先通过修改系统的日志文件，来隐藏自己的行踪，为此我们必须限制对日志文件的访问，禁止一般权限的用户去查看日志文件。当然，系统中内置的日志管理程序功能可能不是太强，我们应该采用专门的日志程序，来观察那些可疑的多次连接尝试。另外，我们还要小心保护好具有根权限的密码和用户，因为黑客一旦知道了这些具有根权限的帐号后，他们就可以修改日志文件来隐藏其踪迹了。 9、使用好登录脚本 制定系统策略和用户登录脚本，对网络用户的行为进行适当的限制。我们可以利用系统策略编辑器和用户登录脚本为用

户设定工作环境，控制用户在桌面上进行的操作，控制用户执行的程序，控制用户登录的时间和地点(如只允许用户在上班时间、在自己办公室的机器上登录，除此以外一律禁止访问)，采取以上措施可以进一步增强系统的安全性。 10、经常检查系统信息 如果在工作的过程中突然觉得计算机工作不对劲时，仿佛感觉有人在遥远的地方遥控你。这时，你必须及时停止手中的工作，立即按 Ctrl Alt Del复合键来查看一下系统是否运行了什么其他的程序，一旦发现有莫名其妙的程序在运行，你马上停止它，以免对整个计算机系统有更大的威胁。但是并不是所有的程序运行时出现在程序列表中，有些程序例如Back Orifice(一种黑客的后门程序)并不显示在Ctrl Alt Del复合键的进程列表中，最好运行“ 附件 ”/“ 系统工具 ”/“ 系统信息 ”，然后双击“ 软件环境 ”，选择“ 正在运行任务 ”，在任务列表中寻找自己不熟悉的或者自己并没有运行的程序，一旦找到程序后应立即终止它，以防后患。 11、对病毒的袭击要警惕 如今病毒在因特网上传播的速度越来越快，为防止主动感染病毒，我们最好不要在Win2000中上网访问非法网站，不要贸然下载和运行不名真相的程序。例如如果你收到一封带有附件的电子邮件，且附件是扩展名为EXE一类的文件，这时千万不能随意运行它，因为这个不明真相的程序，就有可能是一个系统破坏程序。攻击者常把系统破坏程序换一个名字用电子邮件发给你，并带有一些欺骗性主题，骗你说一些：“ 这个东西将给您带来惊喜 ”，“ 帮我测试一下程序 ”之类的话。你一定要警惕了!对待这些表面上很友好、跟善意的邮件附件，我们应该做的是立即删除这些来历不明的文件。 12、设置好系统的安全参数 充分利用NTFS文

件系统的本地安全性能，设计好NTFS文件系统中文件和目录的读写、访问权限，对用户进行分组。对不同组的用户分别授予拒绝访问、读取和更改权限，一般只赋予所需要的最小的目录和文件的权限。值得注意的是对完全控制权限的授予应特别小心。对于网络资源共享，更要设计好文件系统的网络共享权限，对不应共享的文件和目录决不能授予共享权限。对能够共享的文件和目录，应对不同的组和用户分别授予拒绝访问、读、更改和完全控制等权限。