 31.SQL SERVER是NT平台上用的最多的数据库系统，但是它的安全问题也必须引起重视。数据库中往往存在着最有价值的信息，一旦数据被窃后果不堪设想。 及时更新补丁程序。 说明：与NT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。 给SA一个复杂的口令。 说明：SA具有对SQL SERVER数据库操作的全部权限。遗憾的是，一部分网管对数据库并不熟悉，建立数据库的工作由编程人员完成，而这部分人员往往只注重编写SQL 语句本身，对SQL SERVER数据库的管理不熟悉，这样很有可能造成SA口令为空。这对数据库安全是一个严重威胁。目前具有这种隐患的站点不在少数。 严格控制数据库用户的权限，轻易不要给让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。 说明：用户如果对表有直接的操作权限，就会存在数据被破坏的危险。制订完整的数据库备份与恢复策略。 32.目前，PCANYWHERE是最流行的基于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，最好采用加密手段。千万不要采用与NT管理员一样的用户名与口令，也不要使用与NT集成的口令。同时在服务器端的设置时务必采用security options中的强加密方式，拒绝低加密水平的连接，同时采用口令加密与传输过程中的用户名与口令加密，以防止被嗅探到，还要限

制连接次数，另外很重要的一点就是一定在protect item中设置高强度的口令，同时一定限制不能够让别人看到你的host端的任何设置，即便是要察看主机端的相关设置也必须要输入口令！ 说明：PCANYWHERE 口令是远程控制的第一个关口，如果与NT的一样， 就失去了安全屏障。被攻破后就毫无安全可言。而如果采用单独的口令，即使攻破了PCANYWHERE，NT还有一个口令屏障。及时安装较新的版本。 33.实际上，安全和应用在很多时候是矛盾的，因此，你需要在其中找到平衡点，毕竟服务器是给用户用而不是做OPEN HACK的，如果安全原则妨碍了系统应用，那么这个安全原则也不是一个好的原则。 网络安全是一项系统工程，它不仅有空间的跨度，还有时间的跨度。很多朋友（包括部分系统管理员）认为进行了安全配置的主机就是安全的，其实这其中有个误区：我只能说一台主机在一定的情况一定的时间上是安全的随着网络结构的变化、新的漏洞的发现，管理员/用户的操作，主机的安全状况是随时随地变化着的，只有让安全意识和安全制度贯穿整个过程才能做到真正的安全。 以下是提高IIS 5.0网站服务器的执行效率的八种方法： 1. 启用HTTP的持续作用可以改善15~20%的执行效率。 2. 不启用记录可以改善5~8%的执行效率。 3. 使用“ 独立 ”的处理程序会损失20%的执行效率。 4. 增加快取内存的保存文件数量，可提高Active Server Pages之效能。 5. 勿使用CGI程序。 6. 增加IIS 5.0电脑CPU数量。 7. 勿启用ASP侦错功能。 8. 静态网页采用HTTP 压缩，大约可以减少20%的传输量。 