Windows 系统安全设置方法

1、物理安全

服务器应该安放在安装了监视器的隔离房间内，并且监视器要保留 15 天以上的摄像记录。另外，机箱,键盘，电脑桌抽屉要上锁，以确保旁人即使进入房间也无法使用电脑，钥匙要放在另外的安全的地方。

2、停掉 Guest 帐号

在计算机管理的用户里面把 guest 帐号停用掉，任何时候都不允许 guest 帐号登陆系统。为了保险起见，最好给 guest 加一个复杂的密码，你可以打开记事本，在里面输入一串包含特殊字符、数字、字母的长字符串，然后把它作为 guest 帐号的密码拷进去。

3、限制不必要的用户数量

去掉所有的 duplicate user 帐户，测试用帐户，共享帐号，普通部门帐号等等。用户组策略设置相应权限，并且经常检查系统的帐户，删除已经不在使用的帐户。这些帐户很多时候都是黑客们入侵系统的突破口，系统的帐户越多，黑客们得到合法用户的权限可能性一般也就越大。国内的 nt/2000 主机，如果系统帐户超过 10 个，一般都能找出一两个弱口令帐户。我曾经发现一台主机 197 个帐户中竟然有 180 个帐号都是弱口令帐户。

4、创建 2 个管理员用帐号

虽然这点看上去和上面这点有些矛盾，但事实上是服从上面的规则的。 创建一个一般权限帐号用来收信以及处理一些日常事物，另一个拥有 Administrators 权限的帐户只在需要的时候使用。可以让管理员使用

“ RunAS” 命令来执行一些需要特权才能作的一些工作，以方便管理。

5、把系统 administrator 帐号改名

大家都知道，windows 2000 的 administrator 帐号是不能被停用的，这意味着别人可以一遍又一边的尝试这个帐户的密码。把 Administrator 帐户改名可以有效的防止这一点。当然，请不要使用 Admin 之类的名字，改了等于没改，尽量把它伪装成普通用户，比如改成：guestone 。

6、创建一个陷阱帐号

什么是陷阱帐号? Look！创建一个名为“Administrator”的本地帐户，把它的权限设置成最低，什么事也干不了的那种，并且加上一个超过 10 位的超级复杂密码。这样可以让那些 Scripts s 忙上一段时间了，并且可以借此发现它们的入侵企图。或者在它的 login scripts 上面做点手脚。嘿嘿，够损！

7、把共享文件的权限从”everyone”组改成“授权用户”

“everyone” 在 win2000 中意味着任何有权进入你的网络的用户都能够获得这些共享资料。任何时候都不要把共享文件的用户设置成“everyone”组。包括打印共享，默认的属性就是“everyone”组的，一定不要忘了改。

8、使用安全密码

一个好的密码对于一个网络是非常重要的，但是它是最容易被忽略的。前面的所说的也许已经可以说明这一点了。一些公司的管理员创建帐号的时候往往用公司名，计算机名，或者一些别的一猜就到的东西做用户名，然后又把这些帐户的密码设置得 N 简单，比如 “welcome” “iloveyou” “letmein”或者和用户名相同等等。这样的帐户应该要求用户首此登陆的时候更改成复杂的密码，还要注意经常更改密码。前些天在 IRC 和人讨论这一问题的时候，我们给好密码

下了个定义：安全期内无法破解出来的密码就是好密码，也就是说，如果人家得到了你的密码文档，必须花 43 天或者更长的时间才能破解出来，而你的密码策略是 42 天必须改密码。

9、设置屏幕保护密码

很简单也很有必要，设置屏幕保护密码也是防止内部人员破坏服务器的一个屏障。注意不要使用 OpenGL 和一些复杂的屏幕保护程序，浪费系统资源，让他黑屏就可以了。还有一点，所有系统用户所使用的机器也最好加上屏幕保护密码。

10、使用 NTFS 格式分区

把服务器的所有分区都改成 NTFS 格式。NTFS 文件系统要比 FAT,FAT32 的文件系统安全得多。这点不必多说，想必大家得服务器都已经是 NTFS 的了。

11、运行防毒软件

我见过的 Win2000/Nt 服务器从来没有见到有安装了防毒软件的，其实这一点非常重要。一些好的杀毒软件不仅能杀掉一些著名的病毒，还能查杀大量木马和后门程序。这样的话，“黑客” 们使用的那些有名的木马就毫无用武之地了。不要忘了经常升级病毒库

12、保障备份盘的安全

一旦系统资料被破坏，备份盘将是你恢复资料的唯一途径。备份完资料后，把备份盘防在安全的地方。千万别把资料备份在同一台服务器上，那样的话，还不如不要备份。