系统安全：Windows系统安全设置方法(下) 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__E7_B3_BB_E7_BB_9F_E5_AE_89_E5_c100_140054.htm 5.开启密码密码策略 策略 设置 密码复杂性要求 启用 密码长度最小值 6位 强制密码历史 5 次 强制密码历史 42 天 6．开启帐户策略 策略 设置 复位帐户锁定计数器 20分钟 帐户锁定时间 20分钟 帐户锁定阈值 3次 7．设定安全记录的访问权限 安全记录在默认情况下是没有保护的，把他设置成只有Administrator和系统帐户才有权访问。 8．把敏感文件存放在另外的文件服务器中 虽然现在服务器的硬盘容量都很大，但是你还是应该考虑是否有必要把一些重要的用户数据(文件，数据表，项目文件等)存放在另外一个安全的服务器中，并且经常备份它们。 9.不让系统显示上次登陆的用户名 默认情况下，终端服务接入服务器时，登陆对话框中会显示上次登陆的帐户明，本地的登陆对话框也是一样。这使得别人可以很容易的得到系统的一些用户名，进而作密码猜测。修改注册表可以不让对话框里显示上次登陆的用户名，具体是：HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\DontDisplayLastUserName 把 REG_SZ 的键值改成 1 . 10．禁止建立空连接 默认情况下，任何用户通过通过空连接连上服务器，进而枚举出帐号，猜测密码。我们可以通过修改注册表来禁止建立空连接：Local_Machine\System\CurrentControlSet\Control\LSA-RestrictAnonymous 的值改成 ”1 ” 即可。 11.到微软网站下载最新的补丁程序 很多网络管理员没有访问安全站点的习惯，以至于一

些漏洞都出了很久了，还放着服务器的漏洞不补给人家当靶子用。谁也不敢保证数百万行以上代码的2000不出一点安全漏洞，经常访问微软和一些安全站点，下载最新的service pack和漏洞补丁，是保障服务器长久安全的唯一方法。 高级篇： 1. 关闭 DirectDraw 这是C2级安全标准对视频卡和内存的要求。关闭DirectDraw可能对一些需要用到DirectX的程序有影响，但是对于绝大多数的商业站点都应该是没有影响的。修改注册表 HKLM\SYSTEM\CurrentControlSet\Control\GraphicsDrivers\DCI 的Timeout(REG_DWORD)为 0 即可。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com