Windows系统中必须禁止的服务 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/221/2021_2022_Windows_E7_B3_BB_c100_221345.htm 1.NetMeeting Remote Desktop Sharing：允许受权的用户通过NetMeeting在网络上互相访问对方。这项服务对大多数个人用户并没有多大用处，况且服务的开启还会带来安全问题，因为上网时该服务会把用户名以明文形式发送到连接它的客户端，黑客的嗅探程序很容易就能探测到这些账户信息。 2.Universal Plug and Play Device Host：此服务是为通用的即插即用设备提供支持。这项服务存在一个安全漏洞，运行此服务的计算机很容易受到攻击。攻击者只要向某个拥有多台Win XP系统的网络发送一个虚假的UDP包，就可能会造成这些Win XP主机对指定的主机进行攻击（DDoS）。另外如果向该系统1900端口发送一个UDP包，令“ Location ”域的地址指向另一系统的chargen端口，就有可能使系统陷入一个死循环，消耗掉系统的所有资源（需要安装硬件时需手动开启）。 3.Messenger：俗称信使服务，电脑用户在局域网内可以利用它进行资料交换（传输客户端和服务器之间的Net Send和Alerter服务消息，此服务与Windows Messenger无关。如果服务停止，Alerter消息不会被传输）。这是一个危险而讨厌的服务，Messenger服务基本上是用在企业的网络管理上，但是垃圾邮件和垃圾广告厂商，也经常利用该服务发布弹出式广告，标题为“ 信使服务 ”。而且这项服务有漏洞，MSBlast和Slammer病毒就是用它来进行快速传播的。 8.Performance Logs And Alerts：收集本地或远程计算机基于预先配置的日程参数的性能数据，然后将此数据写入日志

或触发警报。为了防止被远程计算机搜索数据，坚决禁止它。 4.Terminal Services：允许多位用户连接并控制一台机器，并且在远程计算机上显示桌面和应用程序。如果你不使用Win XP的远程控制功能，可以禁止它。 5.Remote Registry：使远程用户能修改此计算机上的注册表设置。注册表可以说是系统的核心内容，一般用户都不建议自行更改，更何况要让别人远程修改，所以这项服务是极其危险的。 6.Fast User Switching Compatibility：在多用户下为需要协助的应用程序提供管理。Windows XP允许在一台电脑上进行多用户之间的快速切换，但是这项功能有个漏洞，当你点击“ 开始→注销→快速切换 ”，在传统登录方式下重复输入一个用户名进行登录时，系统会认为是暴力破解，而锁定所有非管理员账户。如果不经常使用，可以禁止该服务。或者在“ 控制面板→用户账户→更改用户登录或注销方式 ”中取消“ 使用快速用户切换 ”。 7.Telnet：允许远程用户登录到此计算机并运行程序，并支持多种 TCP/IP Telnet客户，包括基于 UNIX 和 Windows 的计算机。又一个危险的服务，如果启动，远程用户就可以登录、访问本地的程序，甚至可以用它来修改你的ADSL Modem等的网络设置。除非你是网络专业人员或电脑不作为服务器使用，否则一定要禁止它。 8.Remote Desktop Help Session Manager：如果此服务被终止，远程协助将不可用。 9.TCP/IP NetBIOS Helper：NetBIOS在Win 9X下就经常有人用它来进行攻击，对于不需要文件和打印共享的用户，此项也可以禁用。 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