全面关注Windows系统服务中的安全隐患 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/460/2021_2022__E5_85_A8_E9_9D_A2_E5_85_B3_E6_c100_460808.htm 一、Application Layer Gateway Service（应用层网关服务） 该服务提供因特网联机共享和因特网联机防火墙的第三方通讯协议插件的支持。但是会招致恶意攻击。病毒感染XP系统的应用层网关服务（Application Layer Gateway Service）导致XP系统用户打不开网页。在病毒感染之后，该服务会在每次系统启动时自动启动，并在后台产生一个alg.exe的进程，因此建议禁用该服务。 二、WebClient（网络客户端） 该服务是用来启用Windows为主的程序来建立、存取，以及修改基于Internet的文件默认启动类型为自动。使用WebDav可将档案或数据夹上传到某个Web服务，这个服务对于未来.NET意义更大。但是很容易招致黑客的恶意攻击，建议设为禁用。 三、Distributed Transaction Coordinator（分布式交易协调器） 默认启动类型为手动。主要用来处理分布式交易。同一数据库内不同数据表间的交易，则不能称作分布式交易。显然对于需要同时处理多个数据库或文件系统的用户来说，这个服务意义重大，其实这个服务也容易受到黑客的远程拒绝服务攻击。因此建议设为禁用。 四、Messenger 信使服务发送和接收系统管理员或“ 警报器 ”服务消息的服务。默认启动类型为自动。如果是在同一域中，只需要用NET SEND命令就可以轻易发送消息了。但是"信使服务"不仅会干扰工作，影响心情，而且还容易遭到"社会工程"攻击，很多垃圾邮件发送者都利用这一功能向计算机用户发送垃圾信息。建议设为禁用。 五

、Remote Registry Service 该服务允许远程用户通过简单的连接就能修改本地计算机上的注册表设置。知道管理员账号和密码的人远程访问注册表是很容易的。打开注册表编辑器，选择“ 文件 ”菜单中的“ 连接网络注册表 ”选项，在“ 选择计算机 ”对话框里的“ 输入要选择的对象名称 ”下的输入框中输入对方的IP地址，点击“ 确定 ”按钮便会出现一个“ 输入网络密码 ”对话框，输入管理员账号和密码，点击“ 确定 ”按钮后就可对目标机器的注册表进行修改了。现在，不少木马后门程序可以通过此服务来修改目标机器的注册表，强烈建议大家禁用该项服务。 六、ClipBook 这个服务允许任何已连接的网络中的其他用户查看本机的剪贴板。负责管理这项服务的是网络DDE代理（Network DDE Agent），实际上网络DDE代理会使机器非常容易遭受恶意攻击而失去本机的管理员控制权。因此如果无需ClipBook共享这个特殊服务，不妨禁用。 七、Computer Browser 该服务可以将当前机器所使用网络上的计算机列表提供给那些请求得到该列表的程序(很有可能是恶意程序)，很多黑客可以通过这个列表得知当前网络中所有在线计算机的标志并展开进一步的攻击。建议一般用户禁用该服务。 八、Indexing Service Indexing Service是一个搜索引擎。这个索引服务应该算是多数IIS Web服务器上诸多安全弱点的根源。同时，它也是很多蠕虫病毒爆发的罪魁祸首，例如曾流行一时的红色代码就是利用IIS的缓冲区溢出漏洞和索引服务来进行传播的，而著名的蓝色代码和尼姆达则是分别利用IIS服务的IFRAMEExecCommand、Unicode漏洞来进行传播。因此，如果你不需要架设Web服务器，请一定要关闭该项服务。 九、DNS Client 该服务是用于查询DNS缓存

记录的。可用于对某个已入侵的系统进行DNS查询，可加速DNS查询的速度。攻击者在取得用户的Shell后，可以通过ipconfig/displaydns命令查看用户的缓存内容，获知你所访问过的网站。从而使用户的信息外泄。 十、Server 该服务提供RPC支持以及文件、打印和命名管道共享。Server服务是作为文件系统驱动器来实现的，可以处理I/O请求。如果用户没有提供适当的保护，会暴露系统文件和打印机资源。对于Windows 2000系统而言，这是一个高风险服务。Windows 2000中默认共享的存在就是该服务的问题。如果不禁用该服务，每次注销系统或开机后，默认共享就会打开，你的所有重要信息都将暴露出来。同时，由于很多Windows 2000使用者为了使用方便把管理员密码设置为空密码或非常简单的密码组合，这给了黑客可乘之机。 十一、Workstation 该服务以一个文件系统驱动器的形式工作，并且可以允许用户访问位于Windows网络上的资源。该服务应当只在位于某个内部网络中并受到某个防火墙保护的工作站和服务器上运行。在任何可以连接到Internet的服务器上都应该禁用这个服务，避免信息外露。特别是一些独立服务器(例如Web服务器)是不应当加入到某个Windows网络中的。 十二、TCP/IP NetBIOS Helper Service 在Windows构建的网络中，每一台主机的唯一标志信息是它的NetBIOS名。系统可以利用WINS服务、广播及Lmhost文件等多种模式将NetBIOS名解析为相应IP地址，从而实现信息通讯。在这样的网络内部，利用NetBIOS名实现信息通讯是非常方便、快捷的。但是在Internet上，它就和一个后门程序差不多了。它很有可能暴露出当前系统中的NetBIOS安全性弱点，例如大家所熟悉的139端口入侵就是利用了此服

务。由于NetBIOS是基于局域网的，因此，只需要访问Internet资源的一般用户可以禁用它，除非你的系统处于局域网中。 十三、Terminal Services 该服务提供多会话环境，允许客户端设备访问虚拟的系统桌面会话以及运行在服务器上的基于Windows的程序并打开默认为3389的对外端口，允许外来IP的连接(著名的3389攻击所依靠的服务就是它)。对于这个非常危险的服务，只有“ 禁用 ”。配置服务的方法:进入“ 服务 ”窗口，右键点击要配置的服务，然后点击“ 属性 ”。可根据需要在“ 常规 ”选项卡中，点击“ 自动 ”、“ 手动 ”或“ 已禁用 ”。 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