善用netstat命令化身Windows7安全高手计算机等级考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/645/2021_2022__E5_96_84_E7_94_A8nets_c98_645005.htm 一些基本的命令往往可以在保护网络安全上起到很大的作用，下面几条命令的作用就非常突出。 检测网络连接 如果你怀疑自己的计算机上被别人安装了木马，或者是中了病毒，但是手里没有完善的工具来检测是不是真有这样的事情发生，那可以使用Windows自带的网络命令来看看谁在连接你的计算机。具体的命令格式是：netstat -an 这个命令能看到所有和本地计算机建立连接的IP，它包含四个部分proto(连接方式)、local address(本地连接地址)、foreign address(和本地建立连接的地址)、state(当前端口状态)。通过这个命令的详细信息，我们就可以完全监控计算机上的连接，从而达到控制计算机的目的。 我们在命令提示符中输入如下：netstat -a 显示出你的计算机当前所开放的所有端口 ，netstat -s -e 比较详细的显示你的网络资料，包括TCP、UDP、ICMP 和 IP的统计等大家可能都见过了。那有没有想过更胜层次的了解Vista、Windows7显示协议统计和当前 TCP/IP 网络连接的知识呢？ 软件之家（www.myfiles.com.cn）特别整理netstat命令用法如下（提示：其中按有a-b的顺序排列） NETSTAT：Vista / Windows7 下显示协议统计和当前 TCP/IP 网络连接。可以直接运行netstat不加参数，如图： NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [interval] -a 显示所有连接和侦听端口。 -b 显示在创建每个连接或侦听端口时涉及的可执行程序。在某些情况下，已知可执行程序承载多个独立的组件，这些情况下，显示创建连接

或侦听端口时涉及的组件序列。此情况下，可执行程序的名称位于底部[]中，它调用的组件位于顶部，直至达 到 TCP/IP。注意，此选项可能很耗时，并且在您没有足够权限时可能失败。 -e 显示以太网统计。此选项可以与 -s 选项结合使用。 -f 显示外部地址的完全限定域名(FQDN)。 -n 以数字形式显示地址和端口号。 -o 显示拥有的与每个连接关联的进程 ID。 -p proto 显示 proto 指定的协议的连接；proto 可以是下列任何一个: TCP、UDP、TCPv6 或 UDPv6。如果与 -s 选项一起用来显示每个协议的统计，proto 可以是下列任何一个: IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP或 UDPv6。 -r 显示路由表。 -s 显示每个协议的统计。默认情况下，显示 IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 和 UDPv6 的统计；-p 选项可用于指定默认的子网。 -t 显示当前连接卸载状态。 interval 重新显示选定的统计，各个显示间暂停的间隔秒数。按 CTRL C 停止重新显示统计。 禁用不明服务 很多朋友在某天系统重新启动后会发现计算机速度变慢了，这个时候很可能是别人通过入侵你的计算机后给你开放了特别的某种服务，比如IIS信息服务等。可以通过“ net start ”来查看系统中究竟有什么服务在开启，如果发现了不是自己开放的服务，我们就可以有针对性地禁用这个服务了。方法就是直接输入“ net start ”来查看服务，再用“ net stop server ”来禁止服务。 轻松检查账户 很长一段时间，恶意的攻击者非常喜欢使用克隆账号的方法来控制你的计算机。他们采用的方法就是激活一个系统中的默认账户，但这个账户是不经常用的，然后使用工具把这个账户提升到管理员权限，从表面上看来这个账户还是和原来一样，但是这个克隆的账户却是系统中

最大的安全隐患。恶意的攻击者可以通过这个账户任意地控制你的计算机。为了避免这种情况，可以用很简单的方法对账户进行检测。 首先在命令行下输入net user，查看计算机上有些什么用户，然后再使用“ net user 用户名 ”查看这个用户是属于什么权限的，一般除了Administrator是administrators组的，其他都不是!如果你发现一个系统内置的用户是属于administrators组的，那几乎肯定你被入侵了，而且别人在你的计算机上克隆了账户。快使用“ net user 用户名/del ”来删掉这个用户吧。 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