三个小命令检查电脑是否被安装木马 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/241/2021_2022__E4_B8_89_E4_B8_AA_E5_B0_8F_E5_c100_241130.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。 一、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。 二、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，不管怎么优化都慢，用杀毒软件也查不出问题，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，这样你的杀毒软件是查不出来的。但是别急，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。 三、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! 联网状态下的客户端。对于没有联网的客户端，当其联网之后也会在第一时间内收到更新信息将病毒特征库更新到最新版本。不仅省去了用户去手动更新的烦琐过程，也使用户的计算机时刻处于最佳的保护环境之下。 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