端口知识面面观完全通透了解计算机安全 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/61/2021_2022__E7_AB_AF_E5_8F_A3_E7_9F_A5_E8_c40_61848.htm 每台电脑要与外界网络每建立一个网络连接时，都必须打开电脑中的某个端口。端口就像是电脑与外界网络连接的一扇门，让连接网络成为可能的同时，也带来了许多安全隐患黑客可能通过打开某个端口后门，用木马控制你的电脑.网络病毒也可能在通过端口感染攻击你的电脑…… 一、Windows中的端口查看器 当网速变慢或者出现电脑操作故障时，排除其它原因后，有可能我们已遭受了网络攻击。这时可以查看一下网络端口使用状况。 使用Windows中自带的netstat命令，可以清楚的查看到电脑中打开的端口连接，其格式为:“ netstat -an ”。在显示的信息中包括连接使用的协议、本地和远程计算机的IP地址及连接端口……很多木马和网络病毒都会开放一些特殊的端口，如果在列表中显示一些不常见的端口，也许系统有可能感染了木马或病毒。 二、图形化的端口管理工具 一些图形化的工具可能显得更为简单实用些，TCPView就是一个方便直观的图形化端口连接查看器，可以显示打开的端口及其对应的进程名和进程路径，并可以轻松的关闭某个连接端口。 在TCPView可以清楚的看到某个端口是什么程序所打开的。有的木马常常会伪装成svchost或explorer等系统进程，可以右键点击这些可疑进程，选择“ Process Properties ”命令打开进程属性窗口，在“ Path ”中可以查看到进程的真正路径。如果确定打开此端口的进程是木马的话，直接点击对话窗口中的“ End Process ”按钮即可。 TCPView的端口管理非常强，

除了查看端口，结束非法使用端口的进程外，它还可以直接关闭某个端口的连接。在窗口中右键点击列表中的某个端口进程，选择“ Close Connection ”命令，即可关闭该端口连接而不结束进程。 三、监视端口的一举一动 监视端口实际上就是监视网络连接，有经验的网络安全人员可以通过监视端口，分析各种网络连接入侵等情况。一个自动化的端口监视记录工具，可以有效的帮助我们进行网络入侵分析。 1.使用netstat监视记录端口 “ netstat ”命令也可以完成简单的端口监视功能，执行“ netstat-ano 10>>c:\port.txt ”，即可在C盘下生成名为“ port.txt ”的网络端口状态记录文件，并每隔10秒钟将刷新的状态追加保存在文本中。按下 键，即可中止监视。通过该端口监视记录，可以查看到是否有非法的入侵连接 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