用SSM系统分析软件检测系统打开的端口Microsoft认证考试
 当我们安装软件的时候，如果软件有连接网络的操作，Windows防火墙就会对其进行拦截，并提示我们。尤其是一些单机软件，根本不需要用到网络功能，却被Windows防火墙拦下，那么我们就需要提高警惕了。在Windows XP，Vista以及7中都可以使用同样的办法。但是有些软件本身具有网络功能，例如升级、下载时，那么这招就不好用了。 设置XP防火墙 小贴士：Windows内置防火墙的功能是比较简单的，如果对安全性要求较高，可以选择天网、ZoneAlarm等第三方杀毒软件。 在最新的Windows7中，使用内置的防火墙就足以用来抵抗大部分后门的入侵。在第一次使用Windows7连接上网络之后，会提示选择网络位置，选择为家庭网络即可，在默认设置下就已经开始进行对网络连接进行保护，不需要更多的设置。 查看网络保护状况 如何检测系统打开的端口？ 如果软件已经安装到了系统中，我们该如何检测是否有后门呢？这时我们通过检测系统打开的端口来判别软件是否具有潜在的后门，端口即本机与远程服务器进行连接时所打开的端口。 查看打开的端口 这里我们需要用到一款著名的安全工具IceSword，运行后点击左侧的功能栏处的“ 端口 ”按钮，IceSword会显示当前系统中所有活动的连接，我们可以看到有哪些程序正在与远程服务器进行通信，如果是藏在Windows目录某个角落的文件，或者是文件名比较陌生的程序，那就引起注意了。对于文件名比较陌生的程序，我们可以以其文件名为关键字在“ 百度 ”上进

行搜索，看看该程序是否已经在网络上臭名昭著。 如何监控软件安装行为？ SSM（点击下载）是一款系统分析软件，它可以抽丝剥茧般分析软件的安装行为，无论软件在安装时动了什么小手脚，都逃不过它的眼睛。 不信？让我们来试试，我们以某流氓软件为例。双击流氓软件安装程序，SSM提示explorer.exe尝试启动安装程序，这一步是正常的，但接下去流氓软件的马脚就露出来了。SSM接着提示安装程序尝试启动2027.exe，该文件位于C: emp，2027.exe是什么程序，大家心知肚明。点击“ 允许 ”后，SSM提示注册表关键位置“ User AutoRun ”群组键值被修改，执行这项修改的进程就是2027.exe，修改的目的是将C:WINDOWS\real0update.exe添加进启动项。至此我们已经了解了这个流氓软件的目的：首先运行2027.exe，接着2027.exe会释放一个文件real0update.exe到 C:WINDOWS目录下，并修改注册表使real0update.exe实现开机启动。 查看软件安装时对于系统的修改 SSM的原理是对系统的关键位置进行监控，一旦发现软件有危险的行为就会报警。这样即使软件有后门，要想浑水摸鱼进入系统也不是一件容易的事情。 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