

追踪Windows系统登录时间的三种方法Microsoft认证考试 PDF
转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/581/2021_2022__E8_BF_BD_E8_B8_AAWind_c100_581952.htm

在局域网工作环境中，常常有计算机被他人偷偷攻击，为了寻找幕后攻击黑手，我们需要让Windows系统自动记忆非法攻击者登录系统的时间，以便从中寻找蛛丝马迹。其实，追踪记忆系统登录时间的方法有很多，这不，本文下面提供的几种方法，可以帮助我们随意所欲查看到非法攻击者登录系统的具体时间。1、巧用策略，记录上次登录时间

在多人共同使用同一台计算机的情况下，我们经常会碰到这样一种现象，那就是当自己临时离开计算机的这段时间内，有其他用户偷偷利用自己的账号登录系统，查看自己的操作记录以及其他访问痕迹。为了弄清楚究竟是谁在偷偷关注自己的操作隐私，我们可以利

用Windows Vista系统的组策略设置功能，来自动追踪显示上一次登录系统的时间，同时我们还能顺便查看到究竟是哪个账号偷偷登录了本地计算机系统，下面就是该方法的具体实现步骤

首先打开Windows Vista系统的“开始”菜单，从中点选“运行”命令，在弹出的系统运行对话框中输入

“gpedit.msc”字符串命令，单击“确定”按钮后，进入对应系统的组策略控制台窗口。其次在该控制台窗口的左侧显示窗格中点选“计算机配置”节点选项，再从该节点下面逐一点选“管理模板”/“Windows组件”/“Windows登录选项”项目，同时从“Windows登录选项”项目的右侧显示窗格中找到目标组策略“在用户登录期间显示有关以前登录的信息”，之后用鼠标双击目标组策略选项，打开如图1所示的选项设

置对话框. 检查该对话框中的“已启动”选项是否处于选中状态，如果发现它还没有被选中时，我们只要将它重新选中，再单击“确定”按钮保存好上述设置操作，如此一来本地Windows Vista系统就具有自动记录上次登录系统时间的功能了。完成上面的设置操作后，如果有非法攻击者趁我们不在计算机现场的时候，偷偷利用我们的账号登录计算机时，Windows Vista系统就会自动将非法攻击者登录系统的时间记忆保存下来，下次我们打开计算机输入登录系统的密码时，系统屏幕上就会出现上一次登录系统的具体时间了，同时我们还能看到具体是哪个用户账号执行登录操作的，此时我们可以根据这些状态信息，寻找具体的非法攻击者，确保计算机系统日后不会被继续攻击。

2、巧用脚本，记录本次登录时间

有的时候，我们希望Windows系统能够自动将用户本次登录系统的时间记忆下来，然后对照自己实际的登录时间，如果它们两者之间有明显差别的话，那就说明在自己离开计算机的那一段时间，肯定有人偷偷访问过本地计算机系统了。要记录本次登录时间，我们可以自己动手创建一个系统启动脚本，让其自动显示、保存本次系统登录时间，之后想办法让Windows系统在启动成功后自动执行那个启动脚本就可以了，下面就是具体的实现步骤：首先打开记事本之类的文本编辑程序，在其中输入下面的命令行代码：`@echo off
date /t >t. d:\time.log
time /t >t. d:\time.log` 在确认上面的命令行代码输入无误后，依次单击文本编辑窗口中的“文件”/“保存”命令，将上面的命令代码保存为扩展名为bat的批处理文件，假设在这里我们将该文件取名为“time.bat”，用鼠标双击该批处理文件，系统当前的时间就会被记录保存到

“ d:\time.log ”文件中了. 其次为了让系统在登录成功的时候自动执行“ time.bat ”文件，我们需要将该文件设置为系统启动脚本。在进行这种设置操作时，我们可以依次单击本地系统的“ 开始 ” / “ 运行 ” 命令，在弹出的系统运行对话框中，输入字符串命令“ gpedit.msc ”，单击回车键后，打开对应系统的组策略控制台窗口. 在该控制台窗口的左侧显示区域中，用鼠标逐一点选“ 计算机配置 ” / “ Windows设置 ” / “ 脚本(启动/关机) ” 节点选项，在对应“ 脚本(启动/关机) ” 节点选项的右侧显示区域中，双击“ 启动 ” 项目，打开如图2所示的启动属性设置窗口. 单击该设置窗口中的“ 添加 ” 按钮，从其后出现的文件选择对话框中，选中“ time.bat ” 文件并单击“ 确定 ” 按钮，将其导入到启动脚本列表框中，最后再单击“ 确定 ” 按钮保存好上述设置操作，如此一来Windows系统日后每次启动成功后，都会自动执行“ time.bat ” 批处理文件，而该文件恰好可以将系统启动成功那一刻的时间、日期自动记录保存到“ d:\time.log ” 文件中，到时我们只要查看

“ d:\time.log ” 文件，就能看到本次登录系统的具体时间了。

3、巧用日志，记录每次登录时间 Windows系统具有强大的日志记录功能，善于使用该功能，我们可以让其自动记忆每一次登录系统的具体时间，哪怕是非法攻击者登录本地系统失败了，Windows系统日志也能将其记录下来。在使用日志功能记录每次登录系统时间时，我们需要按照如下步骤进行操作：首先要对系统登录事件进行审核。在默认状态下

，Windows系统不会对系统登录事件进行日志保存操作，只有对该事件进行审核之后，其日志功能才会自动追踪、记忆系统登录事件.在审核系统登录事件时，我们可以依次单击“

开始” / “运行”命令，在弹出的系统运行对话框中，执行字符串命令“secpol.msc”，打开对应系统的本地安全策略窗口。其次在该窗口的左侧位置处依次展开“安全设置” / “本地策略” / “审核策略”分支选项，从目标分支下面双击“审核登录事件”选项，打开如图3所示的设置对话框，选中其中的“成功”、“失败”选项，再单击“确定”按钮保存好上述设置操作。完成上面的设置操作后，Windows系统日后就能自动记录每次登录系统的时间了。如果想查看每次登录系统的时间时，我们可以直接用鼠标右键单击对应系统桌面中的“计算机”图标，从右键菜单中点选“管理”命令，打开对应系统的计算机管理窗口，在该窗口的左侧位置处依次选中“系统工具” / “事件查看器” / “Windows日志” / “系统”分支选项，在目标分支选项下面我们就能看到每次登录系统的具体记录了，双击该记录选项就能查看到具体的登录时间了。

更多优质资料尽在百考试题论坛 百考试题在线题库 微软认证更多详细资料 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