视频 – 记录用户访问（6 分钟）

我们来了解一下更高级的功能。我要将目录更改到 C 驱动器的根目录，然后显示文件的列表。可以看到 C 驱动器上有一个名为 logon.bat 的批处理文件。我用记事本打开此文件。键入 notepad .引用当前文件夹，\ 和我要打开的文件名称，logon.bat。这将在记事本中打开此文件。同样，我打开带有管理特权的命令提示符，该命令提示符将授予我在记事本中对于此文件的管理特权，这是必需的，因为它在 C 驱动器中。我按 Enter 键，这就是我的文件。

现在该文件为 logon.batch 文件。第一行显示备注，发送登录到回滚日志文件。这只是备注。然后下一行是响应，“Log In”一词，并发送日期变量、时间变量和计算机名称变量，并将其追加到 C 驱动器中名为 logins.log 的文件中。我们需要创建此文件。然后我执行相同操作。用日期和时间响应“Log In”，然后不使用计算机名称变量，而使用可变用户。现在这将不起作用。我需要将其更改为用户名，它随后应该能起作用。我会将其追加到 logins.log 文件中。下面我们保存它。然后选择“文件”，“另存为”并将此文件的第二个版本保存为 logoff.bat。我将更改所有文件类型并将其保存然后会将其更改为 logoff，那样就可以跟踪系统上的所有登录和注销，并将其发送出去，也就是将信息设置发送到 logins.log 文件中。我会将其保存然后将其关闭。现在，如果键入 dir 命令，可以看到我有两个文件。我们来创建 logins.log 文件。我将响应一个回滚日志文件。我会将其重定向到名为 logins.log 的文本文件，执行 dir 命令，现在可以看到我有 logins.log 文件和两个批处理文件。

下面打开“组策略编辑器”，键入 gpedit.msc。在“用户配置”下，展开“Windows 设置”，然后展开“脚本”。“脚本”内是“登录”和“注销”，我可以使用它们运行脚本。我可以设置在登录和注销时运行我的批处理文件。我会将我的批处理文件添加到其中。即 logon.bat。然后单击“确定”。再单击“确定”。然后对于注销，我会双击它，并添加我的 logoff.batch 文件。单击两次“确定”。现在，每当用户登录或注销时，都会运行我的批处理文件，然后将该信息发送到我的 logins.log 文件中，这样就拥有了日志文件。单击“确定”，将其关闭，由于更改了组策略设置，因此需要运行组更新或组策略更新。我会使用 /f 这个强制开关。您可以看到正在更新策略。它正在用 gpupdate / f 开关来更新我的组策略。用户策略更新已成功完成，计算机策略更新已成功完成。现在我需要做的就是注销。所以选择“开始”，并在此注销系统。现在重新登录，然后检查我的 logins.log 文件，看看我的两个批处理文件是否已执行。我们可以进入“计算机”，C 驱动器。这是我的 logins.log 文件。而且毫无疑问，要从 Windows 7 PC 注销。注销由学生完成，然后几秒钟后从同一台计算机登录，用户是学生。现在我拥有了回滚日志文件。所以我使用命令行创建文件，移动文件、复制文件而且执行程序并更改本地组策略。您可以看到，很多任务可以通过命令提示符来完成。