卸载补丁去除保护获取Windows2003密码 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/245/2021_2022__E5_8D_B8_E8_BD_BD_E8_A1_A5_E4_c100_245025.htm 命令行下卸载Windows2003 SP1/SP2 %systemroot%\$NtServicePackUninstall$\spuninst\spuninst /U 按无人参与模式删除 service pack。如果使用此选项，那么在卸载 SP1 的过程中，只有出现致命错误才会显示提示。 /Q 按安静模式删除 SP1，此模式与无人参与模式相同，只是隐藏了用户界面。如果使用此选项，那么在卸载 SP1 的过程中不会出现提示。 /Z 卸载 SP1 的过程完成后，不要重新启动计算机。 /F 卸载 SP1 后重新启动计算机时，强制关闭其他应用程序。 因为有的Windows2003在"添加/删除"里没有补丁卸载选择的，所以我利用命令 %systemroot%\$ NtServicePackUninstall$\spuninst\spuninst.exe /Q 在命令行下自动删除，但有的Windows2003机器没有这个SP1/SP2的总目录，比如是如下： C:\WINDOWS\$NtUninstallKB929969$ 的目录 2007-01-11 03:00 spuninst0 个文件 0 字节 C:\WINDOWS\$NtUninstallKB931836$ 的目录 2007-02-18 03:01 spuninst0 个文件 0 字节 那么我们就进一个个目录利用如上方法删除，可以写个批处理程序自动删除。做以上操作只有一个目的，Windows2003 SP0才可以利用findpass从winlogin进程中抓出系统账号明文密码，虽然此方法很暴力，但比有的机器账号密码变态到用pwdump lc5几个月都破不出来要有用，抓出密码也不要忘记重安装上补丁。其实有空可以测试删除哪个小补丁可以findpass出密码，这样的话动作就小很多很多

了，要不然为了保密可能还要帮别人重新打上SP1/SP2。 最后说下Windows2003的findpass工具现在有两种，一个是WinEggDrop写的，一个是www.white-scorpion.nl网站上的。