如何用好winXP的“ 本地安全策略 ” PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/225/2021_2022__E5_A6_82_E4_BD_95_E7_94_A8_E5_c100_225225.htm 单击“ 控制面板→管理工具→本地安全策略 ”后，会进入“ 本地安全策略 ”的主界面。在此可通过菜单栏上的命令设置各种安全策略，并可选择查看方式，导出列表及导入策略等操作。 一、加固系统账户 1.禁止枚举账号 我们知道，某些具有黑客行为的蠕虫病毒，可以通过扫描Windows 2000/XP系统的指定端口，然后通过共享会话猜测管理员系统口令。因此，我们需要通过在“ 本地安全策略 ”中设置禁止枚举账号，从而抵御此类入侵行为，操作步骤如下： 在“ 本地安全策略 ”左侧列表的“ 安全设置 ”目录树中，逐层展开“ 本地策略→安全选项 ”。查看右侧的相关策略列表，在此找到“ 网络访问：不允许SAM账户和共享的匿名枚举 ”，用鼠标右键单击，在弹出菜单中选择“ 属性 ”，而后会弹出一个对话框，在此激活“ 已启用 ”选项，最后点击“ 应用 ”按钮使设置生效。 2.账户管理 为了防止入侵者利用漏洞登录机器，我们要在此设置重命名系统管理员账户名称及禁用来宾账户。设置方法为：在“ 本地策略→安全选项 ”分支中，找到“ 账户：来宾账户状态 ”策略，点右键弹出菜单中选择“ 属性 ”，而后在弹出的属性对话框中设置其状态为“ 已停用 ”，最后“ 确定 ”退出。 下面，我们再查看“ 账户：重命名系统管理员账户 ”这项策略，调出其属性对话框，在其中的文本框中可自定义账户名称(图1)。 二、指派本地用户权利 如果你是系统管理员身份，可以指派特定权利给组账户或单个用户账户。在“ 安全设置 ”

中，定位于“ 本地策略→用户权利指派 ”，而后在其右侧的设置视图中，可针对其下的各项策略分别进行安全设置(图2)。 例如，若是希望允许某用户获得系统中任何可得到的对象的所有权：包括注册表项、进程和线程以及NTFS文件和文件夹对象等(该策略的默认设置仅为管理员)。首先应找到列表中“ 取得文件或其他对象的所有权 ”策略，用鼠标右键单击，在弹出菜单中选择“ 属性 ”，在此点击“ 添加用户或组 ”按钮，在弹出对话框中(图3)输入对象名称，并确认操作即可。 三、活用IP策略 我们知道，无论是木马、后门，还是漏洞、嗅探，大多都是通过端口作为通道。 因此，我们需要关闭那些可能成为入侵通道的端口。你可以上网查询一下相关危险端口的资料，以做到有备而战。其端口屏蔽方法参见2003年《电脑报》第43期E13版。 四、加强密码安全 在“ 安全设置 ”中，先定位于“ 账户策略→密码策略 ”，在其右侧设置视图中，可酌情进行相应的设置，以使我们的系统密码相对安全，不易破解。如防破解的一个重要手段就是定期更新密码，大家可据此进行如下设置：鼠标右键单击“ 密码最长存留期 ”，在弹出菜单中选择“ 属性 ”，在弹出的对话框中，大家可自定义一个密码设置后能够使用的时间长短(限定于1至999之间)。 此外，通过“ 本地安全设置 ”，还可以进行通过设置“ 审核对象访问 ”，跟踪用于访问文件或其他对象的用户账户、登录尝试、系统关闭或重新启动以及类似的事件。诸如此类的安全设置，不一而足。大家在实际应用中会逐渐发觉“ 本地安全设置 ”的确是一个不可或缺的系统安全工具。 