南開大學

《信息对抗技术》课程实验报告

实验三：Windows 账户和密码的安全设置

学　　院　网络空间安全学院

专　　业　信息安全

学　　号　2112060

姓　　名　孙蕗

一、实验目的

Windows 作为使用最为广泛的桌面操作系统，其安全性尤为重要，在保障其安全运行的所有措施中，其中账户的密码的安全设置是最基本的一个环节。因为账户和密码是系统登录的基础防线，也是众多黑客程序攻击和窃取的对象。普通用户常常在安装系统后长期使用系统的默认设置，忽略了 Windows 系统默认设置的不安全性，而这些不安全性常常被攻击者所利用来得到系统的账户，进一步破解密码。因此，保障系统账户的密码的安全是十分重要的。

二、实验内容

熟练掌握 Windows 账户和密码安全设置方法。

三、实验环境

VMware Windows XP 虚拟机

四、实验原理

1. 设置密码

在设置密码的时候建议让密码的复杂度越高越好，而且尽量不要用简单易猜测的数字组合作为密码选择，在我的计算机中，密码一般采用字母、数字、符号混合使用的方式设定。

2. 删除不再使用的账户，禁用 Guest 账户

共享账户、Guest 账户因为安全保护级别较弱，易受到黑客攻击，系统的账户越多，被攻击者攻击的可能性就越大，因此需要我们及时删除和禁用这些潜在受攻击可能性的账户。

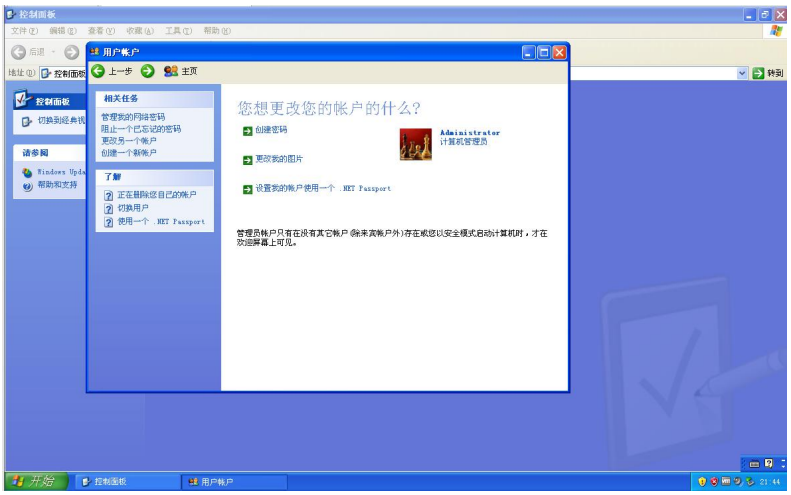
3. 启用账户策略

在控制面板的管理工具中，我们可以选择设置账户策略中的密码策略，来决定系统密码的安全规则和设置。符合复杂性要求的密码是具有相当长度，同时含有数字、大小写字母和特殊字符的序列。双击其中的每一项，可以按照需要改变密码特性的设置。

五、实验过程

1. 设置密码

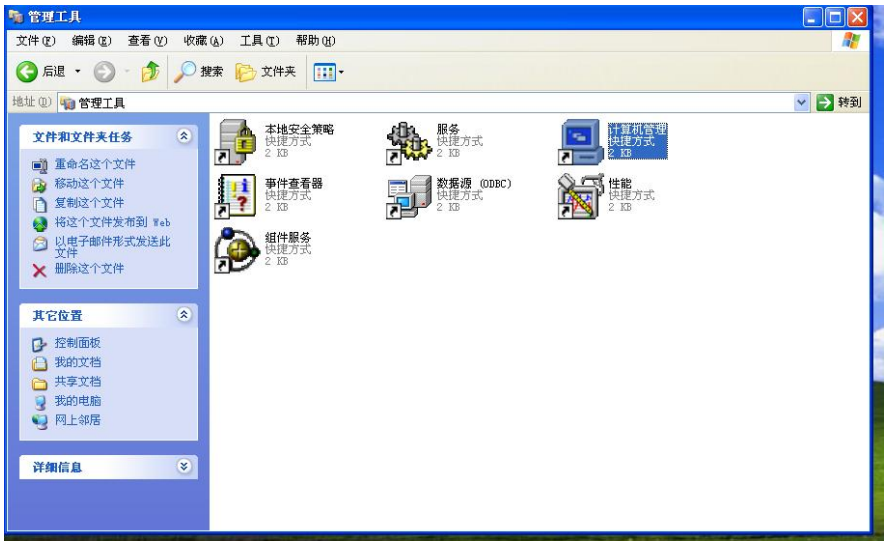
点开“控制面板“中的”用户账户“，挑选计算机管理员账户做更改，点击“创建密码”，为管理员账户创建密码。

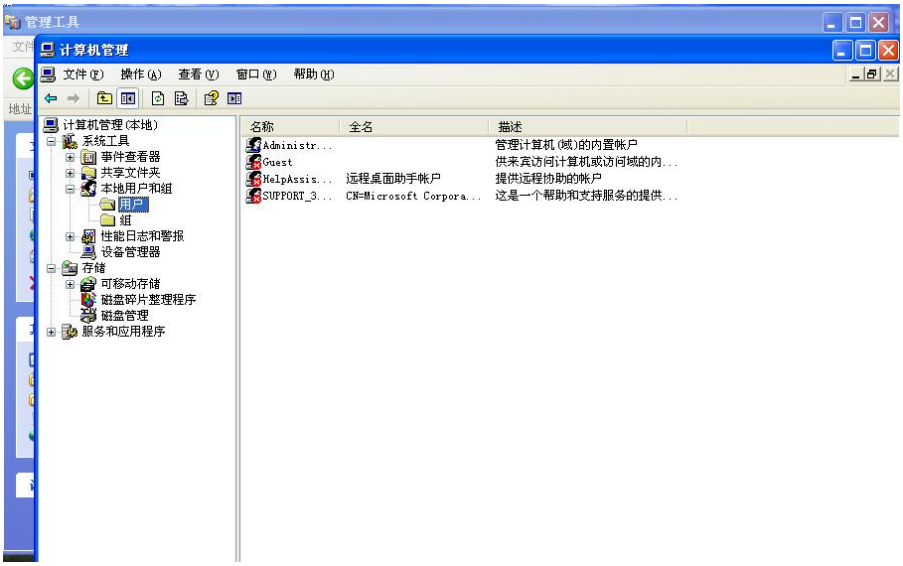


2. 删除不再使用的账户，禁用 Guest 账户

1) 检查和删除不必要的账户

在 Window XP 中，打开控制面板，选择性能和维护，选择“管理工具”中的“计算机管理”，选中 “本地用户和组”，打开“用户”，弹出如下图所示窗口。

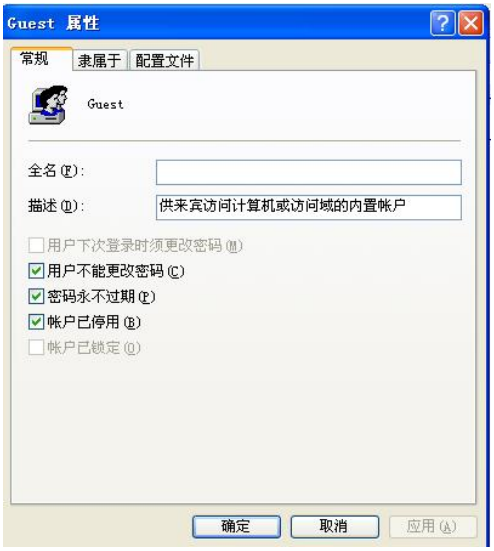




弹出的窗口中列出了系统所有的账户，确认这些账户是否仍在使用，并删除其中不用的账户。

2）Guest 账户禁用

选中 Guest 账户，在右键菜单中选择“属性”命令，弹出如下图所示对话框。 选中“账户已停用”复选框。

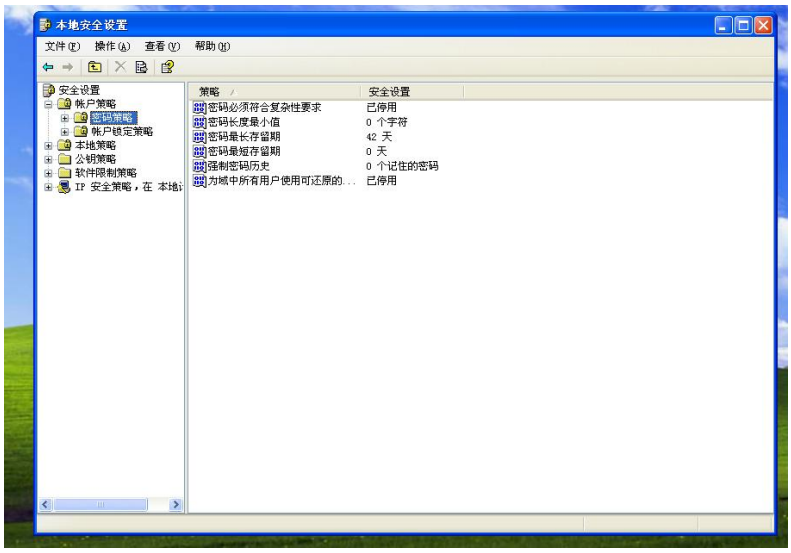


确定后，Guest 账户所对应的图标上会出现一个红色的叉。此时再用 Guest 账户登录，则会显示“您的账户已停用，请与管理员联系”。

图中显示已经删除了不必要的账户和禁用了 Guest 用户。

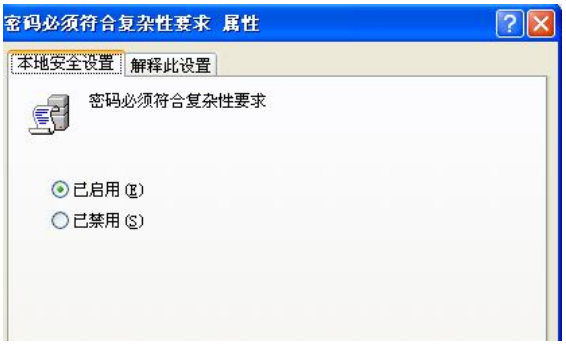
3. 启用账户策略

用快捷键 win+R 打开“运行”，输入“secpol.msc“进入本地安全策略，在弹出的窗口中选择账户策略->密码策略。密码策略用于决定系统密码的安全规则和设置。符合复杂性要求的密码是具有相当长度，同时含有数字、大小写字母和特 殊字符的序列。双击其中的每一项，按照需要改变密码特性的设置。



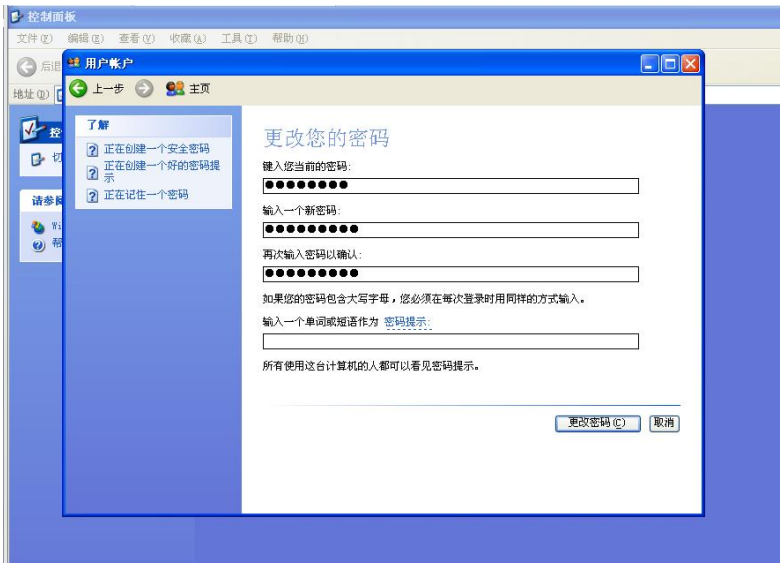
(1) 启用密码必须符合复杂性要求

双击密码必须符合复杂性要求，在弹出的对话框中选择已启用。



点开控制面板中的用户账户，在弹出的对话框中选择一个账户，以管理员账户为例，为管理员账户创建密码。

单击创建密码按钮，在出现的设置密码窗口中输入密码。此时设置的密码要符合所设定的策略。



（2） 设置密码长度最小值

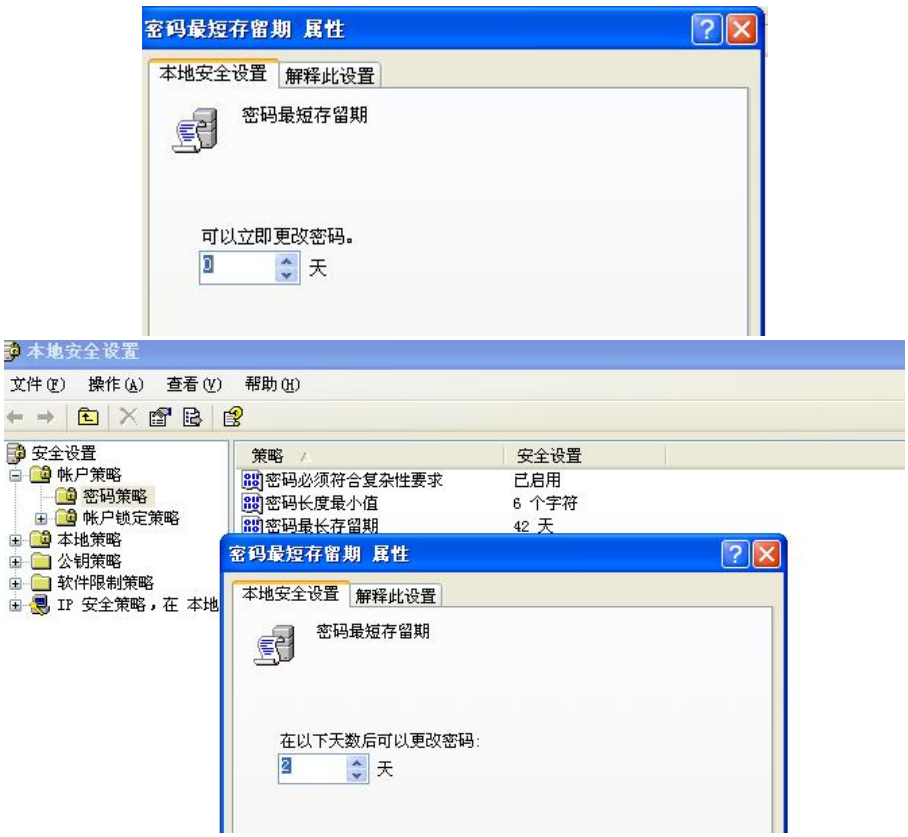
在刚才的密码策略页面中双击密码长度最小值，在弹出的如下图所示的对话框中设置可被系统接纳的账户密码长度最小值。

（3） 设置密码最长存留期

在刚才的密码策略页面中双击密码最长存留期，在弹出的如下图所示的对话框中设置密码最长存留期。设置密码自动保留期，可以提醒用户定期修改密码，防止密码使用时间过长带来的安全问题。

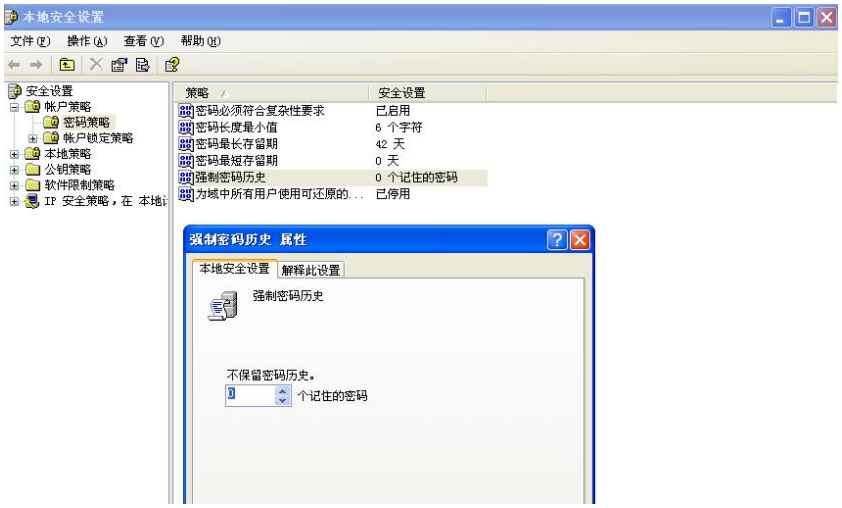
（4） 设置密码最短存留期

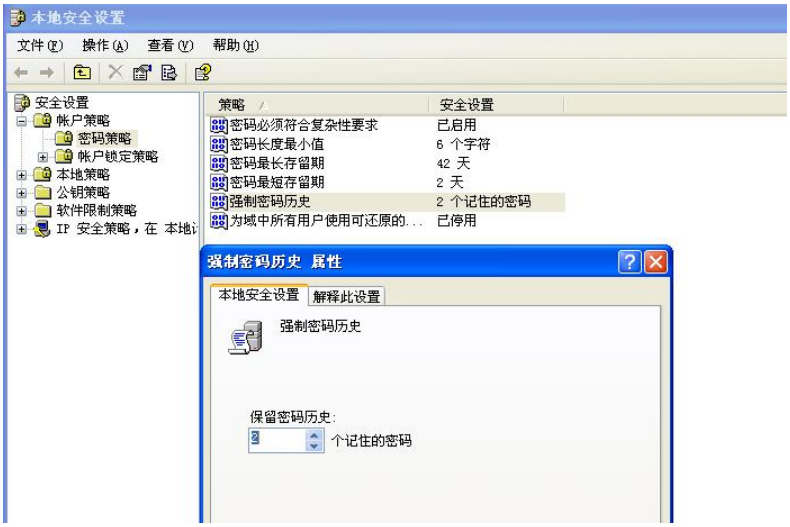
在刚才的密码策略页面中双击密码最短存留期，在弹出的如下图所示的对话框中设置密码最短存留期。在密码最短存留期内不能修改密码。这项设置是为了避免入侵攻击者修改账户密码，其中 0 天表示可以立即更改密码。



（5） 设置强制密码历史

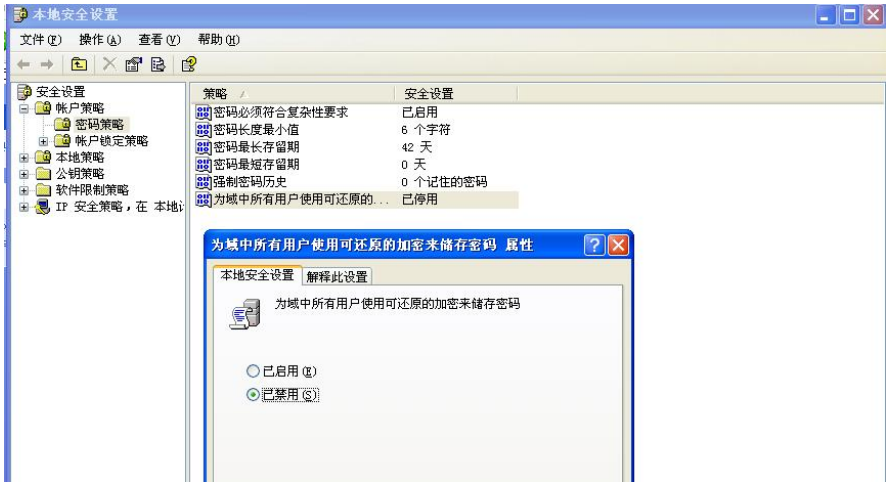
在刚才的密码策略页面中双击强制密码历史，在弹出的如下图所示的对话框中设置让系统记住的密码数量，其中 0 表示不保留密码历史记录。





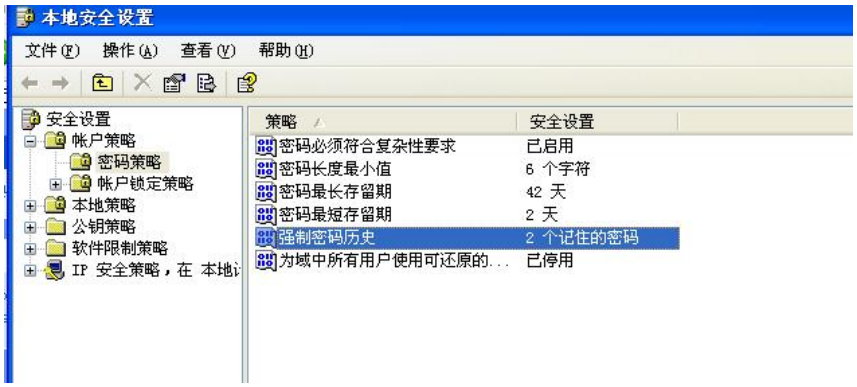
（6） 设置为域中所有用户使用可还原的加密来储存密码

在刚才的密码策略页面中双击为域中所有用户使用可还原的加密来储存密码，在弹出的如下图所示的对话框中设置是否使用可还原的加密来存储密码。



完成密码策略的设置。

设置后各项如下图所示



windows 账户和密码的安全设置就完毕了。

六、实验结论及心得体会

本次实验通过在 Windows XP 虚拟机环境下，对账户密码的安全设置进行了实践操作，从而加深了对 Windows 账户安全性管理的理解。实验内容包括设置复杂密码、删除不再使用的账户、禁用 Guest 账户以及启用账户策略等多个方面，旨在通过这些操作提高系统的安全性。

通过本次实验，我深刻认识到了密码复杂度对于账户安全的重要性。一个强密码应包含字母、数字和特殊字符的组合，且长度足够，以抵御简单的暴力破解攻击。此外，定期更换密码、设置密码历史和存留期限等措施，可以有效防止密码被猜测或复用，从而增强账户的安全性。实验中，我还学习到了如何通过管理工具中的账户策略来设置密码规则，这些规则包括密码必须符合的复杂性要求、密码的最小长度、密码的最长和最短存留期以及强制密码历史记录等。这些设置可以帮助管理员强制执行密码策略，确保所有用户账户都遵循一定的安全标准。

此外，实验还涉及到了账户的管理，如删除不必要的账户和禁用 Guest 账户。这些操作有助于减少潜在的安全风险，因为每一个账户都可能成为攻击者的目标。通过减少系统中的账户数量，可以有效降低被攻击的风险。

总之，本次实验不仅让我掌握了 Windows 账户和密码的安全设置方法，还让我意识到了在日常使用计算机时，应该采取哪些措施来保护账户安全。这些知识和技能对于提高个人和组织的信息安全具有重要意义。