

准备工作

打开 Windows 实验台，运行 Windows 2003 系统。

任务一：进行 Windows 操作系统的帐户策略管理

(1) 实验操作者以管理员身份登录系统：打开“控制面板|管理工具”，运行“本地安全策略”；打开“本地安全设置”对话框，选择“帐户策略|密码策略|密码长度最小值”，通过此窗口设置密码长度的最小值，如下图所示。



选择“密码必须符合复杂性要求”，通过此窗口可以启用此功能，如图所示：



(2) 实验操作者以管理员身份登录系统：打开“控制面板|管理工具”，运行“本地安全策略”；打开“本地安全设置”对话框，选择“帐户策略|帐户锁定策略|帐户锁定阈值”，如图所示。



任务二：Windows 操作系统中文件操作的审计策略

(1) 实验操作者以管理员身份登录系统：打开“控制面板|管理工具”，运行“本地安全策略”；打开“本地安全设置”对话框，选择“本地策略|审核策略”，双击“审核对象访问”，选“成功”和“失败”，如图所示。



(2) 在硬盘上新建一个名为“测试保密.vsd”文件，右键单击该文件，单击“属性”，然后单击“安全”选项卡。如图所示。



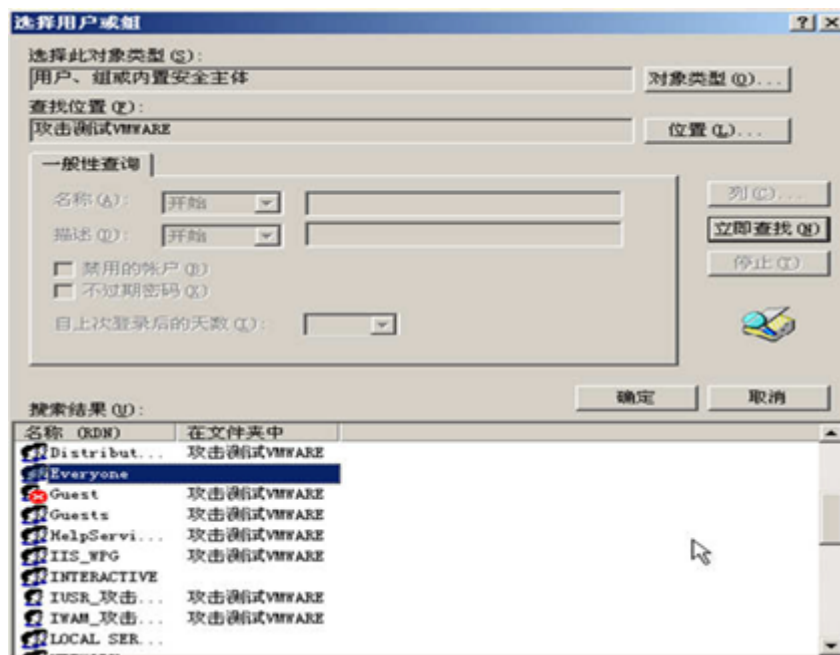
(3) 单击“高级”，然后单击“审核”选项卡。如图所示。



(4) 单击“添加”；在“输入要选择的对象名称”中，键入“Everyone”，然后单击“确定”。如图所示。



单击“高级”，选择“Everyone”如图所示：



(5) 在“测试保密.vsd 的审核项目”对话框中，选择访问中的“删除”和“更改权限”的功能；如图所示。



至此，对“测试保密.vsd”的审计设置完后，删除此文件。如图所示。



(6) 右键单击桌面上“我的电脑”，选择“管理”，在计算机管理中，选择“系统工具|事件查看器|安全性”，或在“开始|运行”中执行 `eventvwr.exe`，应该能看到。如图所示。



任务三：对 Windows 用户账号管理进行审计

(1) 打开“控制面板|管理工具”，运行“本地安全设置”；选择“安全设置|本地策略|审核管理”，双击“审核帐户管理”，选“成功”和“失败”。如图所示。



(2) 在“开始|运行”中，输入 `cmd`，在控制台下输入创建用户 `myTest` 和设置口令的命令，如图所示。



```
C:\WINDOWS\system32\cmd.exe

C:\>net user myTest /add
命令成功完成。

C:\>net user myTest 123456
命令成功完成。
```

(3) 在“开始|运行”中执行 `eventvwr.exe`，在打开的“事件查看器”窗口中选择“安全性”，或右键单击桌面上“我的电脑”，选择“管理”，在计算机管理中，选择“系统工具| 事件查看器|安全性”，可以看到如图所示的记录：



类型	日期	时间	来源	分
审核成功	2008-8-20	17:24:42	Security	对
审核成功	2008-8-20	17:24:42	Security	对
审核成功	2008-8-20	17:22:19	Security	对
审核成功	2008-8-20	17:22:19	Security	帐
审核成功	2008-8-20	17:22:19	Security	帐
审核成功	2008-8-20	17:22:19	Security	对
审核成功	2008-8-20	17:22:03	Security	对
审核成功	2008-8-20	17:22:03	Security	对

双击审计日志，可以看到如下图所示事件记录



事件 属性

事件详细信息

日期 (A): 2008-8-20 来源 (S): Security
时间 (M): 17:22:19 类别 (C): 帐户管理
类型 (T): 审核成功 事件 ID (I): 642
用户 (U): 攻击测试VMWARE\Administrator
计算机 (C): 攻击测试VMWARE

描述 (D):

更改了用户帐户:

目标帐户名称: myTest
目标域: 攻击测试VMWARE
目标帐户 ID: 攻击测试VMWARE\myTest
调用方用户名: Administrator
调用方所属域: 攻击测试VMWARE
调用方登录 ID: {0x0, 0x18584}
特权: -

数据 (D): C /字节 (B) C /字 (W)

确定 取消 应用 (A)

任务四：对 Windows 用户登录事件进行审计

(1) 运行“本地安全设置”，选择“安全设置|本地策略|审计策略”，双击“审核帐户登录事件”，选“成功”和“失败”，如图所示。



(2) 注销当前用户，并能从新登录，登录输入密码是第一次输错密码，第二次输入正确密码，进入系统。

(3) 在“开始|运行”中执行 eventvwr.exe；或右键单击桌面上“我的电脑”，选择“管理”，在计算机管理中，选择“系统工具|事件查看器|安全性”；在打开的“事件查看器”窗口中选择“安全性”，可以看到如图所示的记录。



(4) 双击审计日志，应可以看到如下两图所示的事件记录。



任务五：对 IE 浏览器进行安全配置

(1)安全区域设置

指定 Web 站点为本地 Intranet 站点、可信站点或受限站点

在 IE“工具”菜单上，点击“Internet 选项”，选择“安全”选项卡，然后选择将要把 Web 站点指定到的安全区域：本地 Intranet、可信站点或受限站点（默认情况下所有站点都属于 Internet 区域），如图所示。



点击“站点”按钮，输入 Web 站点地址点击“添加”按钮，如图所示。



改区域的安全级别 在“安全”选项卡上选择要更改其安全级别的区域，点击“自定义级别...”按钮，进行自定义设置。具体如图所示。



(2)自动完成配置

IE 浏览器默认打开自动完成功能，在 Internet 选项中选择“内容”标签页，点击“自动完成”按钮，如图所示。



在弹出的“自动完成设置”窗口中点击“清除表单”和“清楚密码”按钮，也可以取消上方复选框的选择以停用自动完成功能，如图所示。



任务六：对系统补丁自动升级进行配置

选择“我的电脑”，右键“属性”。在弹出的系统“属性窗口”中选择“自动更新”标签页，如图所示。

