<table>
<tr><td>课程名称</td><td colspan="2">保密技术基础 A</td><td>实验课时</td><td>4</td></tr>
<tr><td>实验项目
名称
和序号</td><td>Windows 操作系统安全</td><td>3</td><td>同组者
姓　名</td><td>无</td></tr>
<tr><td>实验目的
及要求</td><td colspan="4">实验目的
通过实验掌握 Windows 账户与密码的安全设置、文件系统的保护和加密、安全策略与安全模板的使用、审核和日志的启用、本机漏洞检测软件 MBSA 的使用，建立一个 Windows 操作系统的基本安全框架。

实验要求
根据教材中介绍的 Windows 操作系统的各项安全性实验要求，详细观察并记录设置前后系统的变化，给出分析报告。</td></tr>
<tr><td>实验环境</td><td colspan="4">1 台安装 Windows2000/XP 操作系统的计算机，磁盘格式配置为 NTFS，预装 MBSA(Microsoft Baseline Security Analyzer)工具</td></tr>
<tr><td>实验内容</td><td colspan="4">实验内容：

1. 账户与密码的安全设置
2. 文件系统的保护和加密
3. 启用安全策略与安全模板
4. 用加密软件 EFS 加密硬盘数据
5. 审核与日志查看
6. 利用 MBSA 检查和配置系统安全
需要说明的是，下面的实验步骤主要是以 Windows2000 的设置为例进行说明，并且设置均需以管理员（Administrator）身份登陆系统。在 Windows XP 或其他操作系统中，相关安全设置会稍有不同，但大同小异。</td></tr>
</table>

实验步骤

方　　法

关键代码

实验步骤：

任务一　账户和密码的安全设置

1．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

右键单击“开始”按钮，打开“资源管理器”，选择“控制面板”中的“用户和密码”项；在弹出的对话框中列出了系统的所有账户。确认各账户是否仍在使用，删除其中不用的账户。如下图一所示：

图一 查看用户账户

（2）禁用 guest 账户

为了便于观察实验结果，确保实验用机在实验前可以使用 guest 账户登陆。打开“控制面板”中的“管理工具”，选中“计算机管理”中“本地用户和组”，打开“用户”，右键单击 guest 账户，在弹出的对话框中选择“属性”，在弹出的对话框中“帐户已停用”一栏前打勾。

确定后，观察 guest 前的图标变化（图二），并再次试用 guest 用户登陆，记录显示的信息（图三）。

图二 更改 guest 停用对比

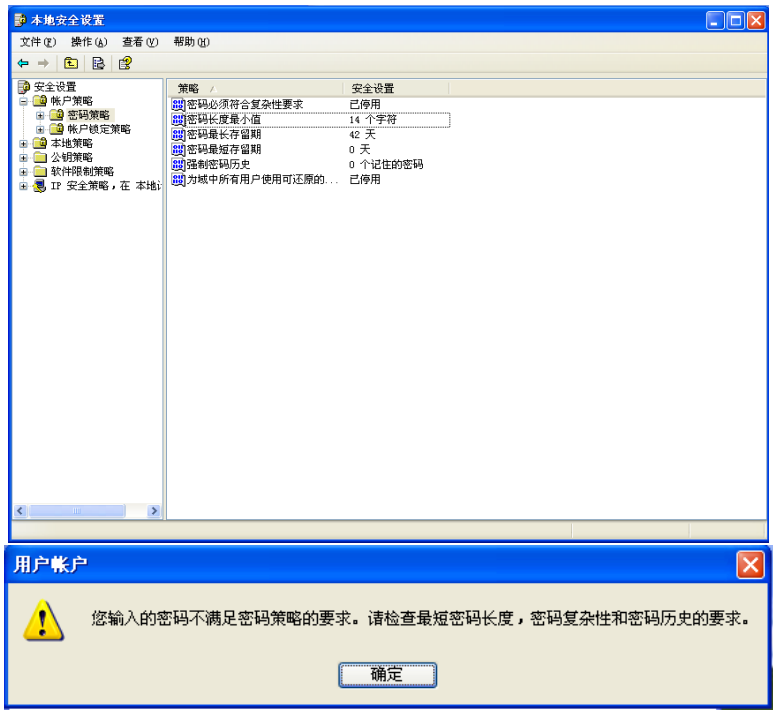
当 guest 账户禁用时，进行切换 guest 账户，会提示启用账户。

图三 禁用 guest 并进行用户登陆

2. 启用账户策略

（1）设置密码策略

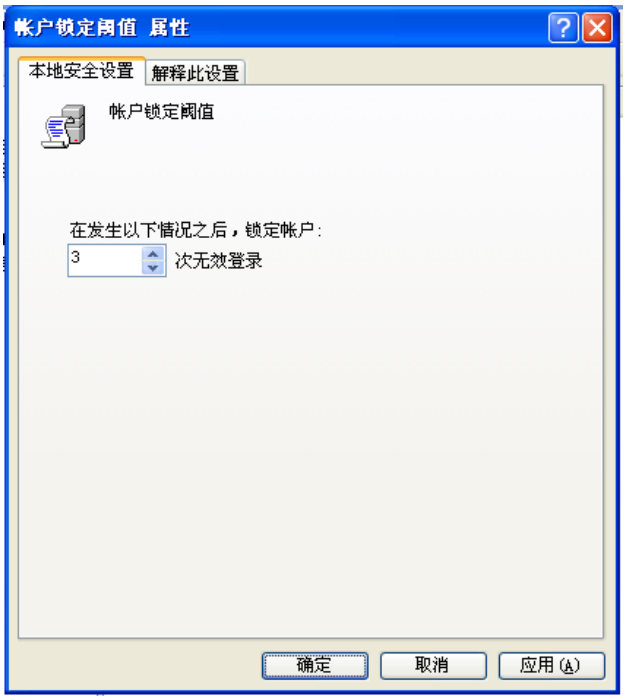
打开“控制面板”中的“管理工具”，在“本地安全策略”中选择“账户策略”；双击“密码策略”，在右窗口中，双击其中每一项，可按照需要改变密码特性的设置。根据你选择的安全策略，尝试对用户的密码进行修改以验证策略是否设置成功，记录下密码策略和观察到的实验结果（图四）。



图四 设置密码策略并修改密码

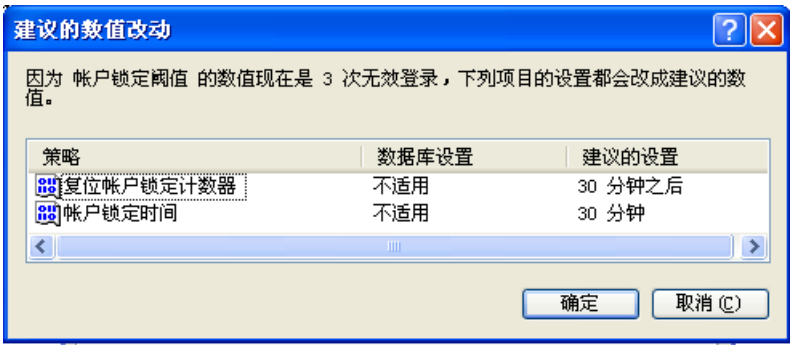
（2）设置账户锁定策略

打开“控制面板”中的“管理工具”，在“本地安全策略”中选择“账户策略”。双击“帐户锁定策略”。在右窗口中双击“账户锁定阀值”，在弹出的对话框中设置账户被锁定之前经过的无效登陆次数（如 3 次），以便防范攻击者利用管理员身份登陆后无限次的猜测账户的密码，见图五。



图五账户锁定阀值设置

在右窗口中双击“账户锁定时间”，在弹出的对话框中设置账户被锁定的时间（如 20 min），见图六。



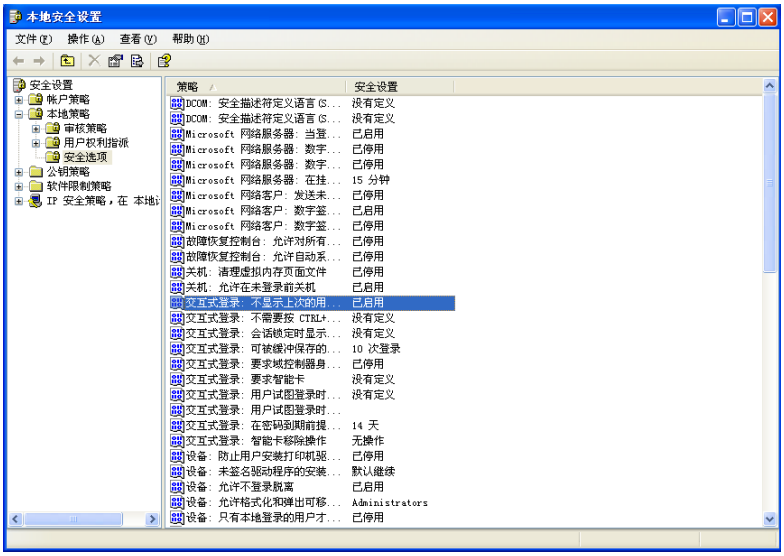
图六 账户锁定时间设置

重启计算机，进行无效的登陆（如密码错误），当次数超过 3 次时，记录系统锁定该账户的时间，并与先前对“账户锁定时间”项的设置进行对比。用户锁定信息见图七。

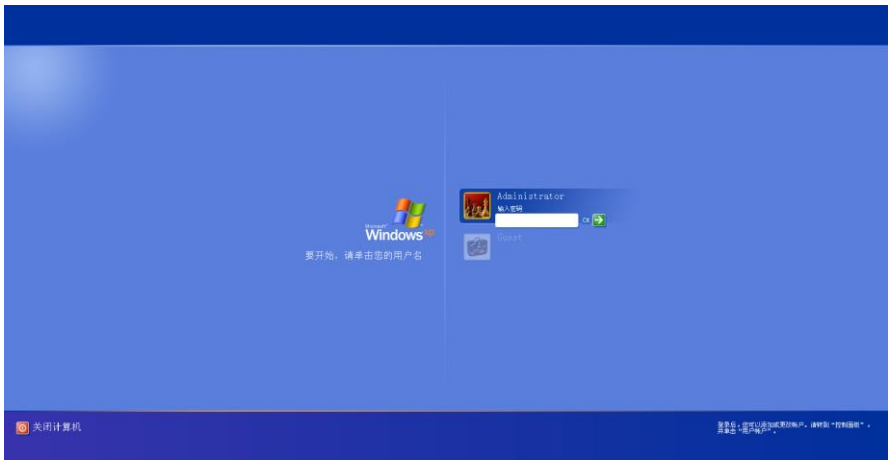
图七 账户锁定信息

3. 开机时设置为“不自动显示上次登陆账户”

右键单击“开始”按钮，打开“资源管理器”，选中“控制面板”，打开“管理工具”选项，双击“本地安全策略”项，选择“本地策略”中的“安全选项”，并在弹出的窗口右侧列表中选择“登陆屏幕上不要显示上次登陆的用户名”选项，启用该设置（图八）。设置完毕后，重启机器看设置是否生效，见图九。



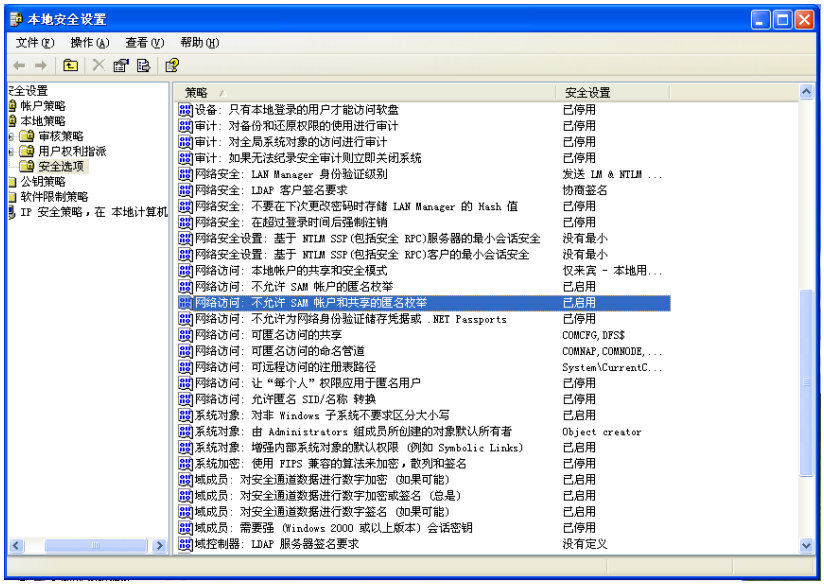
图八 启用“不显示上次登陆的用户名”选项



图九 验证设置生效

4．禁止枚举账户名

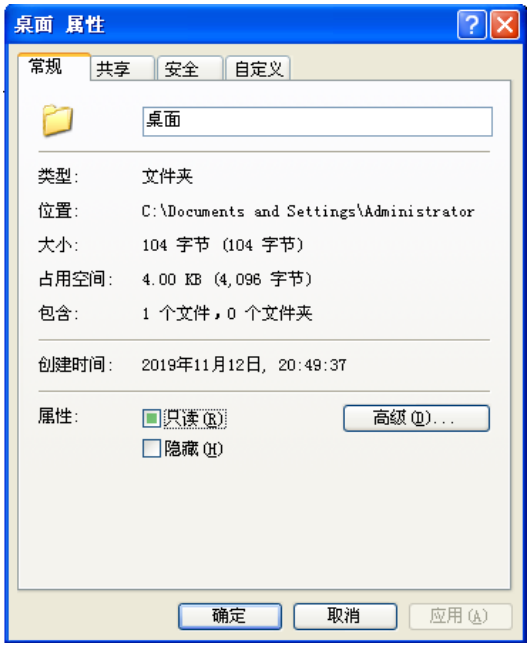
右键单击“开始”按钮，打开“资源管理器”，选中“控制面板”，打开“管理工具”选项，双击“本地安全策略”项，选择“本地策略”中的“安全选项”，并在弹出的窗口右侧列表中选择“对匿名连接的额外限制”项，在“本地策略设置”中选择“不允许枚举 SAM 账户和共享”（图十）。



图十 “不允许枚举 SAM 账户和共享”设置

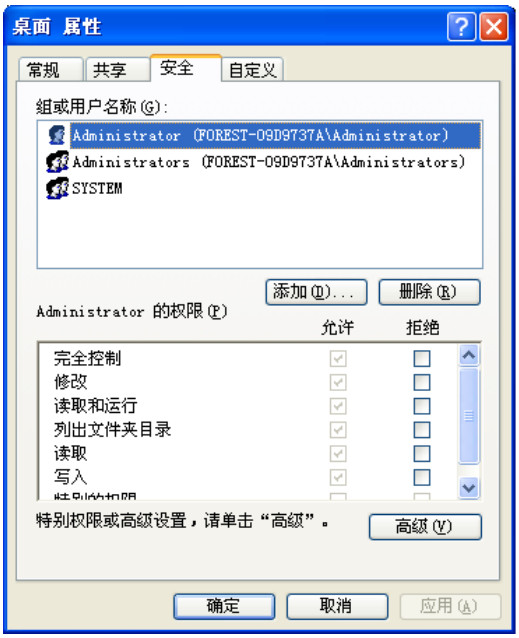
任务二 文件系统安全设置

（1）打开采用 NTFS 格式的磁盘，选择一个需要设置用户权限的文件夹。这里选择 E 盘下的“桌面”文件夹，见图十一。



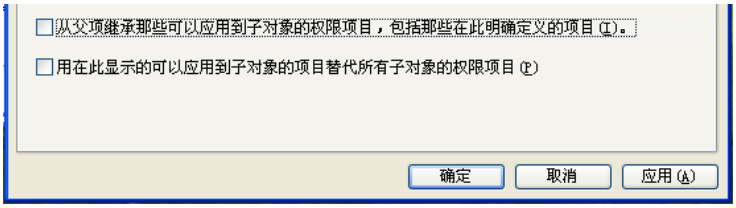
图十一 桌面文件夹属性

（2）右键单击该文件夹，选择“属性”，在工具栏中选择“安全”，见图十二。



图十二 桌面文件夹下的安全选项

（3）将“允许来自父系的可能继承权限无限传播给该对象”之前的勾去掉（图十三），以去掉来自父系文件夹的继承权限（如不去掉则无法删除可对父系文件夹操作用户组的操作权限）。

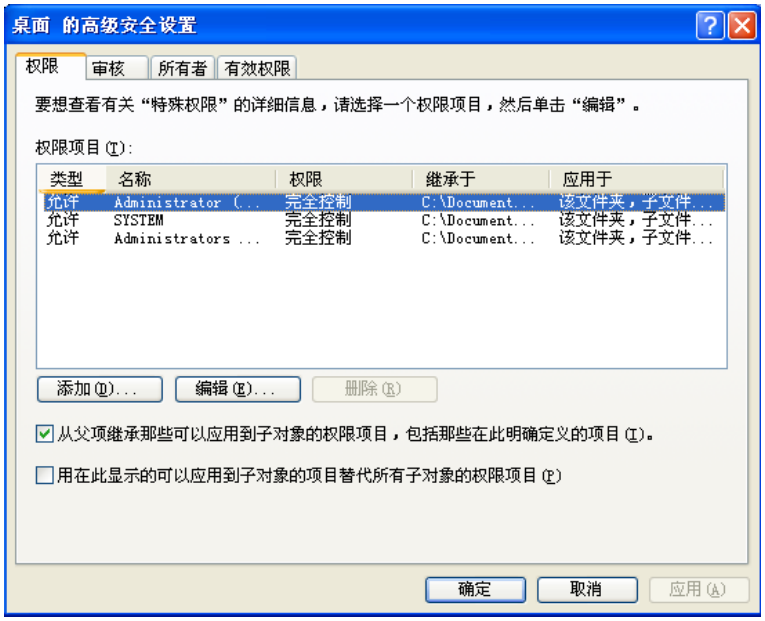


图十三 取消“允许来自父系的可能继承权限无限传播给该对象”

（4）选中列表中的 Everyone 组，单击“删除”按钮，删除 Everyone 组的操作权限，由于新建的用户往往都归属于 Everyone 组，而 Everyone 组在缺省情况下对所有系统驱动器都有完全控制权，删除 Everyone 组的操作权限可以对新建用户的权限进行限制，原则上只保留允许访问此文件夹的用户和用户组。

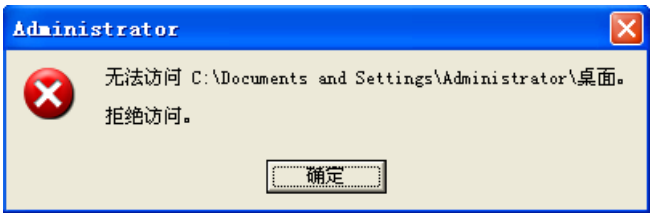
（5）选择相应的用户组，在对应的复选框中打勾，设置其余用户组对该文件夹的操作权限。

（6）单击“高级”按钮，在弹出的窗口中，查看各用户组的权限，见图十四。



图十四 各用户组的权限

（7）注销计算机，用不同的用户登陆，查看 E 盘“桌面”文件夹的访问权限，当不具有权限的用户访问时，结果记录见图十五。



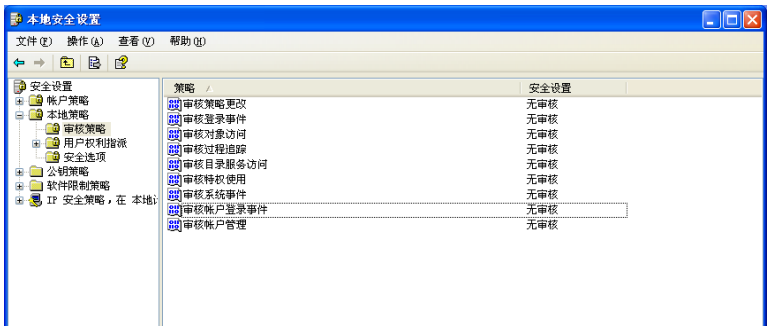
图十五 访问提示信息

任务三　启用审核与日志查看

1. 启用审核策略

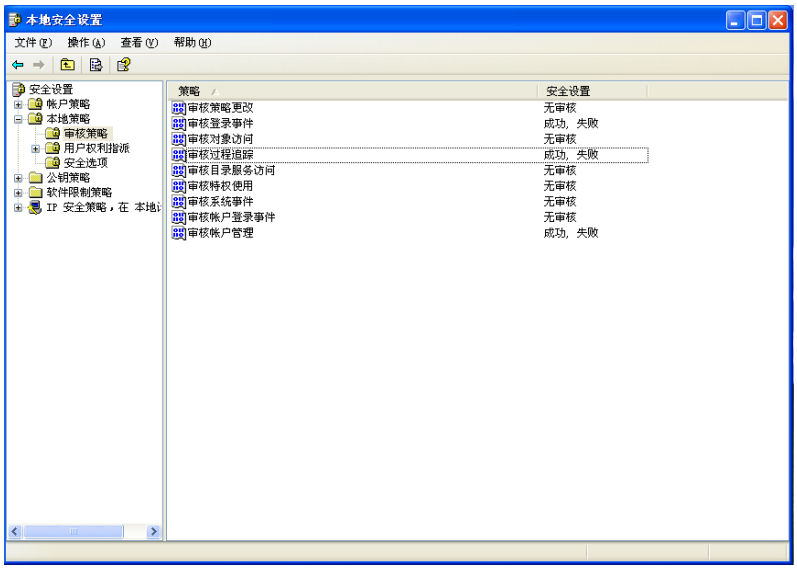
（1）打开“控制面板”中的“管理工具”，选择“本地安全策略”。

（2）打开“本地策略”中的“审核策略”，在实验报告中记录当前系统的审核策略，见图十六。



图十五 当前系统的审核策略

（3）双击每项策略可以选择是否启用该项策略，例如“审核账户管理”将对每次建立新用户、删除用户等操作进行记录，“审核登陆事件”将对每次用户的登陆进行记录；“审核过程追踪”将对每次启动或者退出的程序或者进程进行记录，根据需要启用相关审核策略（图十六），审核策略启用后，审核结果放在各种事件日志中。



图十六 启用相关审核策略

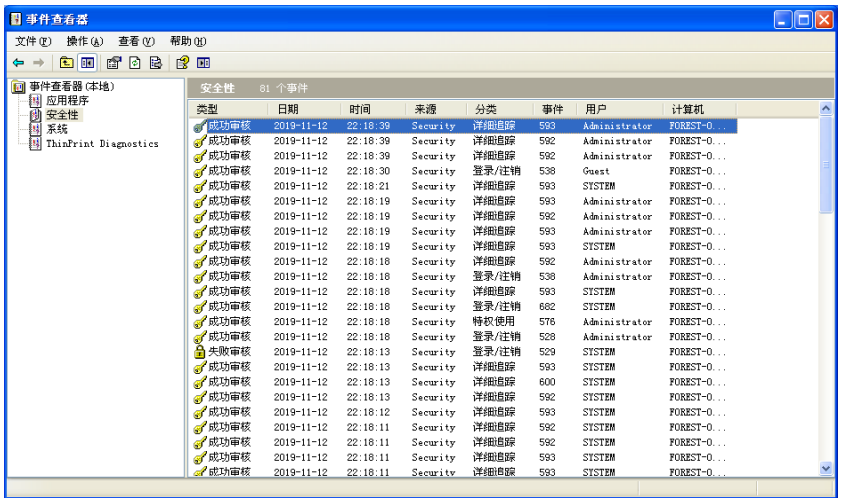
2. 查看事件日志

（1）打开“控制面板”中的“管理工具”，双击“事件查看器“，在弹出的窗口中查看系统的 3 种日志，见图十七。

图十七 系统的 3 种日志

（2）双击“安全日志”，可查看有效无效、登陆尝试等安全事件的具体记录（图十八），

例如： 查看用户登陆/注销的日志。



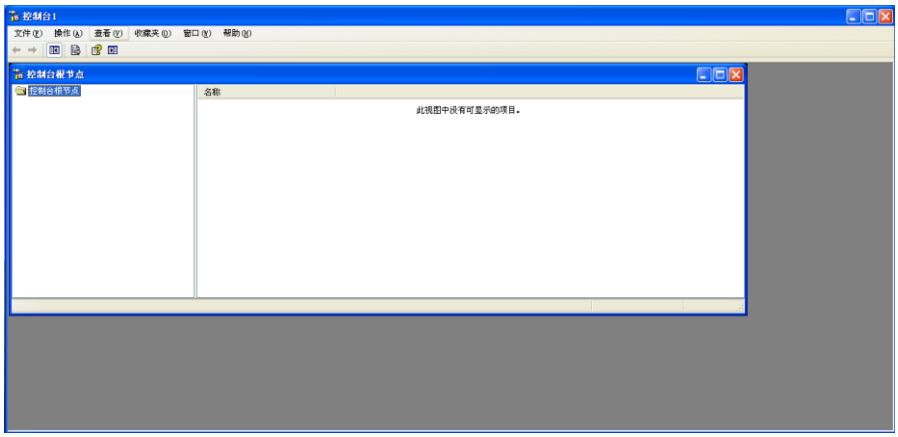
图十八 查看安全日志

任务四 启用安全策略与安全模块

1. 启用安全模板

开始前，请记录当前系统的账户策略和审核日志状态，以便于同实验后的设置进行比较。

（1）单击“开始”按钮，选择“运行”按钮，在对话框中运行 mmc，打开系统控制台，见图十九。

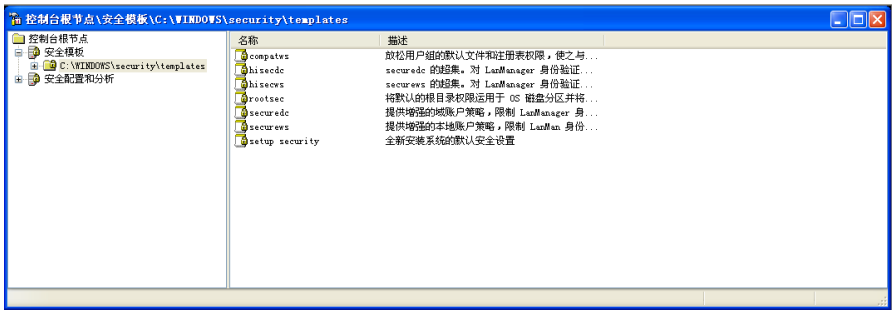


图十九 系统控制台

（2）单击工具栏上“控制台”，在弹出的菜单中选择“添加/删除管理单元”（图二十），单击“添 加”，在弹出的窗口中分别选择“安全模板”、“安全设置和分析”，单击“添加”按钮 后，关闭窗口，并单击“确定”按钮。

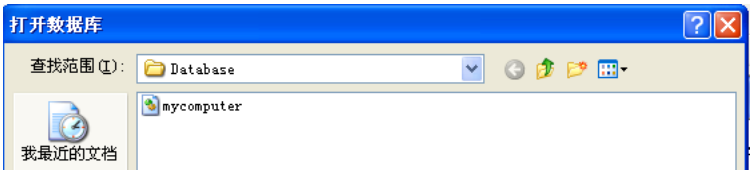
图二十添加/删除管理单元

（3）此时系统控制台中根节点下添加了“安全模板”、“安全设置分析”两个文件夹，打开“安全模板”文件夹，可以看到系统中存在的安全模板。右键单击模板名称，选择“设置描述”，可以看到该模板的相关信息。选择“打开”，右侧窗口出现该模板的安全策略，双击每中安全策略可看到其相关配置，见图二十一。



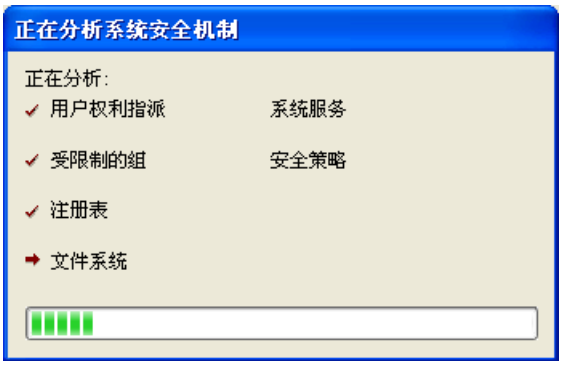
图二十一 安全模板的相关策略

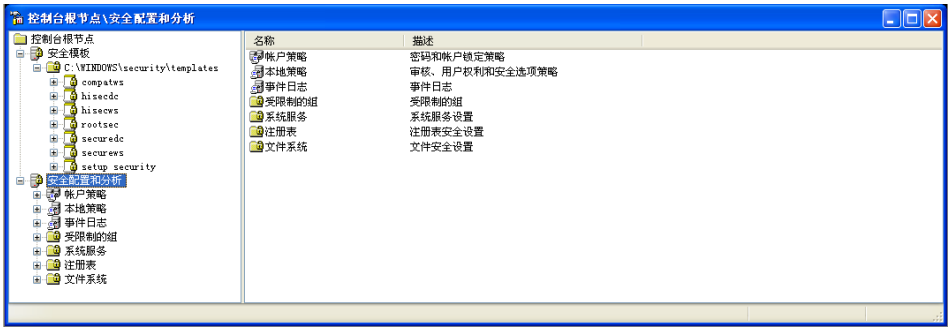
（4）右键单击“安全设置与分析”，选择“打开数据库”。在弹出的对话框中输入预建安全数据库的名称，例如起名为 mycomputer.sdb（图二十二），单击“打开”按钮，在弹出的窗口中，根据计算机准备配置成的安全级别，选择一个安全模板将其导入。



图二十二 建立安全数据库

（5）右键单击“安全设置与分析”，选择“立即分析计算机”，单击“确定”按钮，系统开始按照上一步中选定的安全模板，对当前系统的安全设置是否符合要求进行分析，见图二十三。

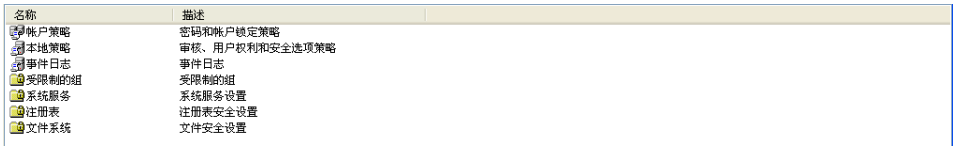




图二十三 计算机分析结果

（6）右键单击“安全设置与分析”，选择“立即配置计算机”，则按照第（4）步中所选的安全模板的要求对当前系统进行配置。

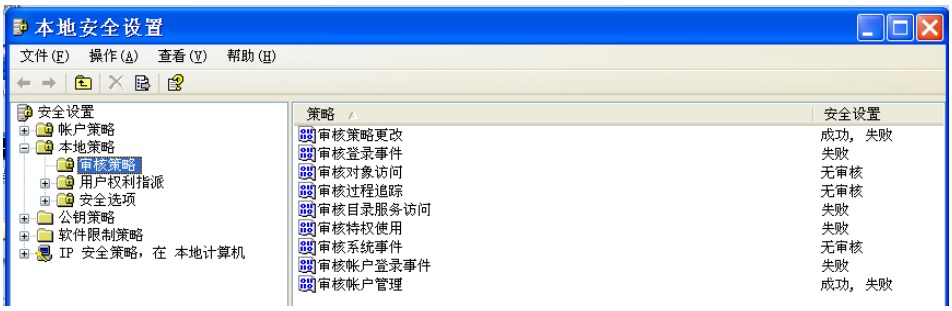
（7）在实验报告中记录实验前系统的缺省配置，接着记录启用安全模板后系统的安全设置（图二十四），记录下比较和分析的结果。



名称	描述
帐户策略	密码和帐户锁定策略
本地策略	审核、用户权利和安全选项策略
事件日志	事件日志
受限制的组	受限制的组
系统服务	系统服务设置
注册表	注册表安全设置
文件系统	文件安全设置

图二十四 启用安全模板后系统安全社会

按照步骤配置完计算机之后，再次查看账户策略和审核策略，发现很多项已经发生改变了，和安全模板的设置一样，也就是说系统按照模板对安全策略进行了配置（图二十五）。

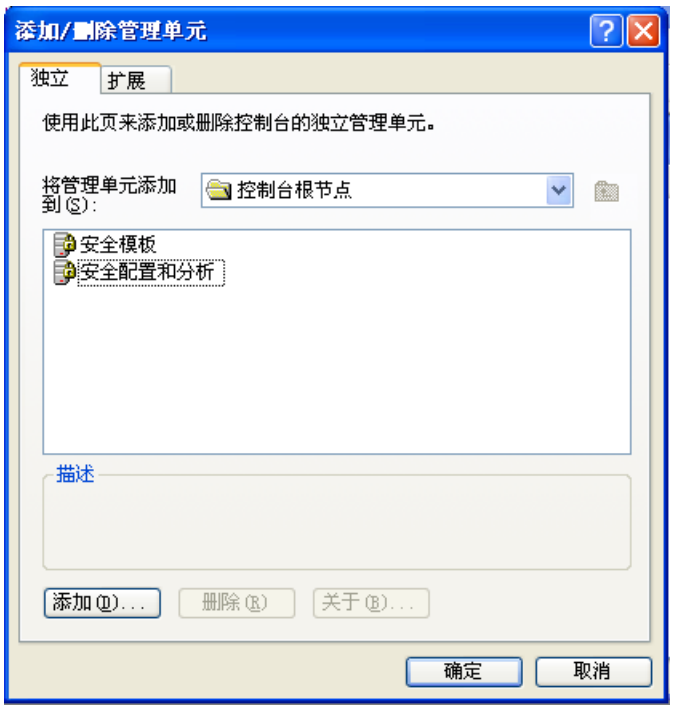


图二十五 模板安全配置设置

2. 建安全模板

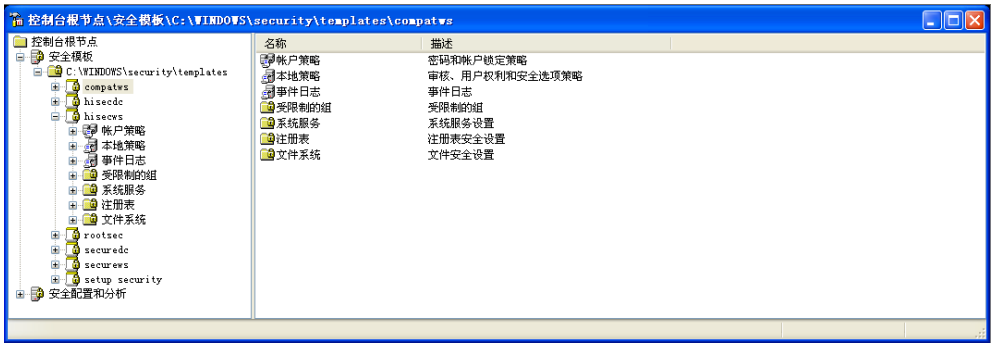
（1）单击“开始”按钮，选择“运行”按钮，在对话框中运行 mmc，打开系统控制台。

（2）单击工具栏上“控制台”，在弹出的菜单中选择“添加/删除管理单元”，单击“添加”，在弹出的窗口中分别选择“安全模板”、“安全设置和分析”，单击“添加”按钮后，关闭窗口，并单击“确定”按钮，见图二十六。



图二十六 添加管理单元

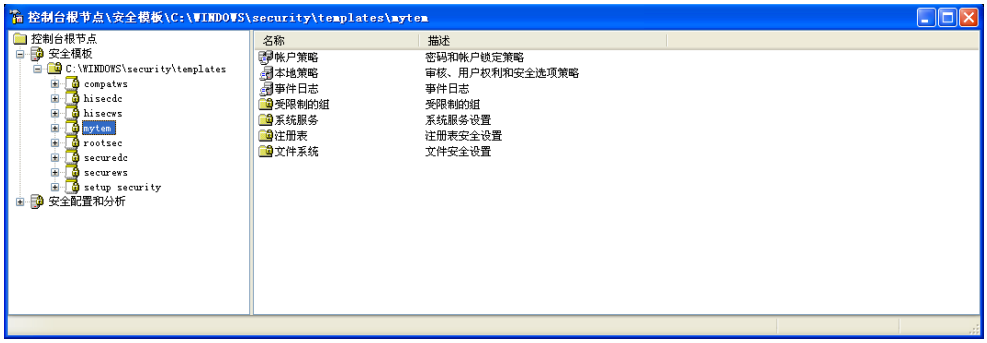
（3）此时系统控制台中根节点下添加了“安全模板”、“安全设置分析”两个文件夹，打开“安全模板”文件夹，可以看到系统中存在的安全模板。右键单击模板名称，选择“设置描述”，可以看到该模板的相关信息。选择“打开”，右侧窗口出现该模板的安全策略，双击每中安全策略可看到其相关配置（图二十七）。



图二十七 安全策略相关配置

（4）右键单击“安全设置与分析”，选择“打开数据库”。在弹出的对话框中输入预建安全数据库的名称，例如起名为 mycomputer.sdb，单击“打开”按钮，在弹出的窗口中，根据计算机准备配置成的安全级别，选择一个安全模板将其导入。

（5）展开“安全模板”，右键单击模板所在路经,选择“新加模板”，在弹出的对话框中添如预加入的模板名称 mytem，在“安全模板描述“中填入“自设模板”。查看新加模板是否出现在模板列表中，见图二十八。

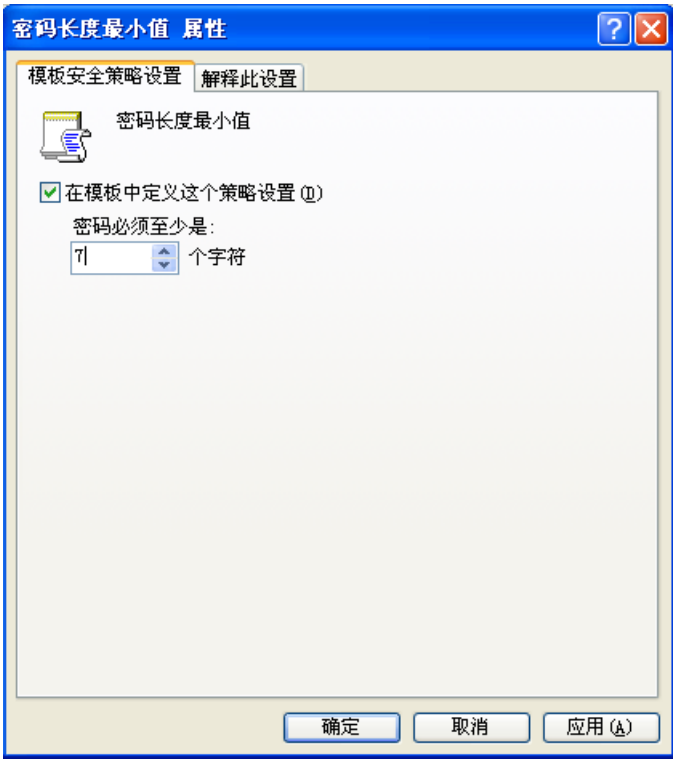


图二十八 自建模板

（6）双击 mytem，在现实的安全策略列表中双击“账户策略”下的“密码策略”，可发现其中任一项均显示“没有定义”，双击预设置的安全策略（如“密码长度最小值”），弹出如图二十九所示的窗口。

（7）在“在模板中定义这个策略设置”前打勾，在框中填如密码的最小长度为 7。

（8）依次设定“账户策略”、“本地策略”等项目中的每项安全策略，直至完成安全模板的设置。

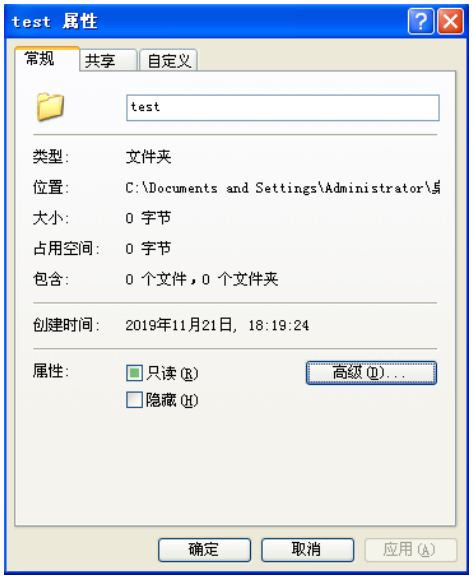


图二十九 安全策略设置

任务五 利加密软件 EFS 加密硬盘数据

（1）打开“控制面板”中的“用户和密码”，创建一个名为 MYUSER 的新用户。

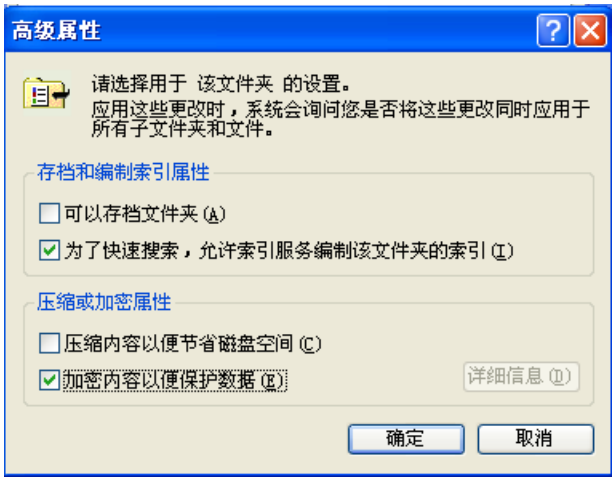
（2）打开硬盘格式为 NTFS 的磁盘，选择要进行加密的文件夹（以 test 文件夹为例），见图三十。



图三十 选择加密文件夹

（3）右键单击该文件夹，打开“属性”窗口，选择“常规”，单击“高级”按钮。

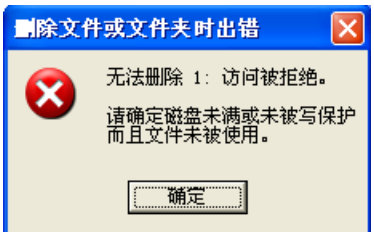
（4）选择“加密内容以便保护数据”，单击“确定”按钮（图三十一）。



图三十一 加密内容

（5）在弹出的对话框中选择“将更改利用于该文件夹、子文件夹和文件”。

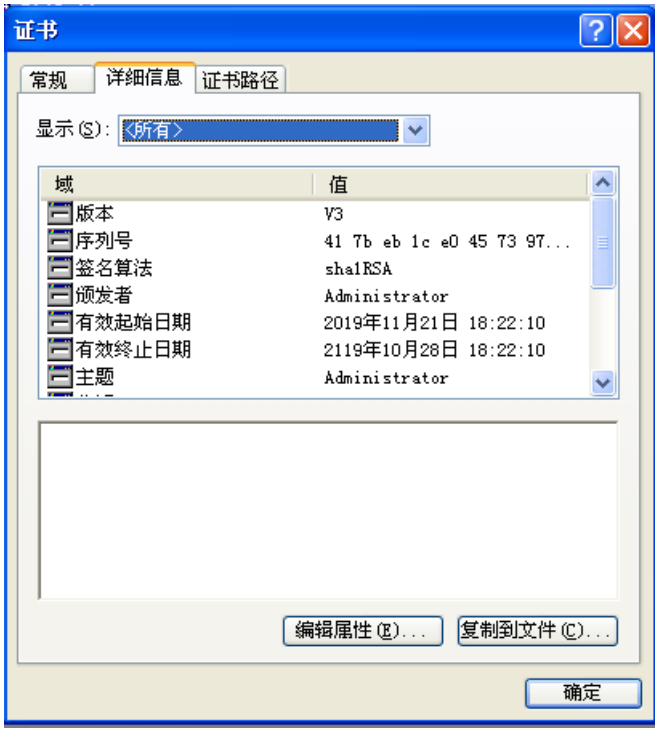
（6）加密完成后，保存当前用户下的文件，单击“开始”按钮，打开“关机”，在下拉列表中选择“注销…用户”(即当前用户)，以刚才新建的 MYCOMPUTER 用户登陆系统，再次访问“工具备份”文件夹，结果见图三十二。



图三十二 访问结果

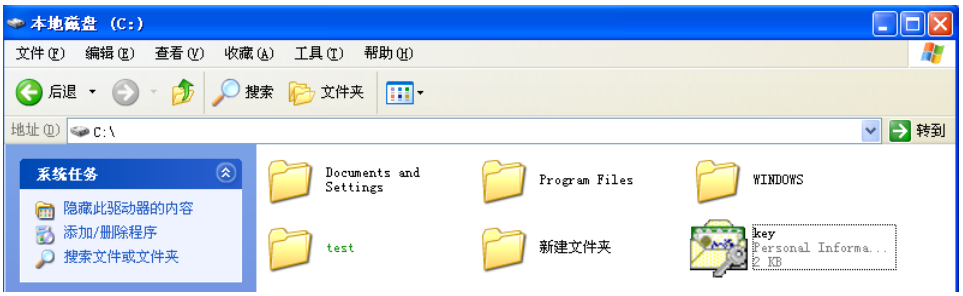
（7）再次切换用户，以原来加密文件夹的管理员用户登陆系统，单击“开始”按钮，在“运行”框输入 mmc，打开系统控制台。单击左上角的“控制台”按钮，选择“添加/删除管理单元”，在弹出的对话框中单击“添加”按钮，选择添加“证书”，为当前的加密文件系统 EFS 设置证书。

（8）在控制台窗口左侧的目录树中选择“证书”“个人“证书”。可以看到用于加密文件系统的证书显示在右侧的窗口中。双击此证书，单击详细信息，则可以看到此证书包含的详细信息，记录这些信息，见图三十三。



图三十三 证书信息

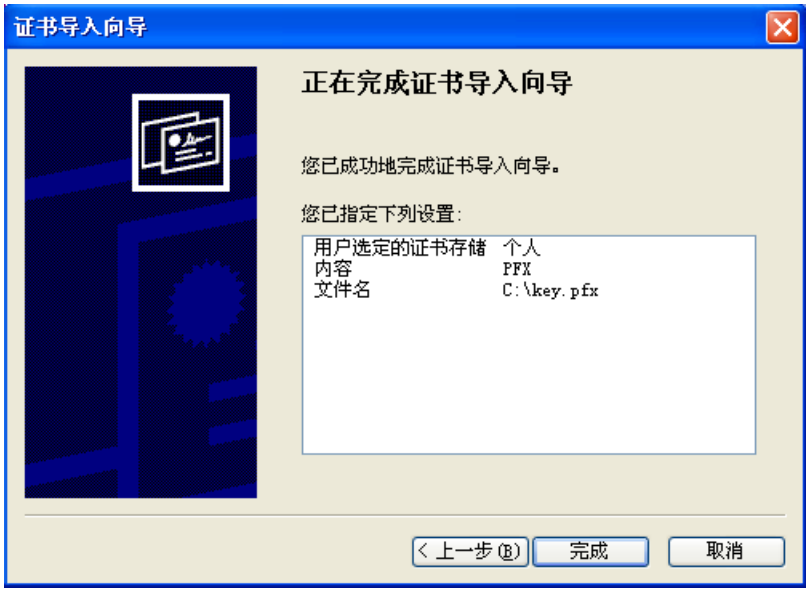
（9）选中用于 EFS 的证书，单击右键，在弹出的菜单中单击“所有任务”，在展开的菜单中，单击“导出”，则弹出“欢迎使用证书导出向导”，单击“下一步”按钮，选择“是”，导出私钥”，接着设置保护私钥的密码，然后将导出的证书文件保存在磁盘上的某个路经，这就完成了证书的导出，见图三十四。



图三十四 证书的导出

（10）再次切换用户，以新建的 MYCOMPUTER 登陆系统，重复步骤（7）和（8），右键单击选中的“证书”文件夹，选择“所有任务”中的“导入”，在弹出的“使用证书导入向导”窗口中，单击“下一步”按钮，在地址栏中填入步骤（9）中导出证书文件夹的地址，导入该证书。

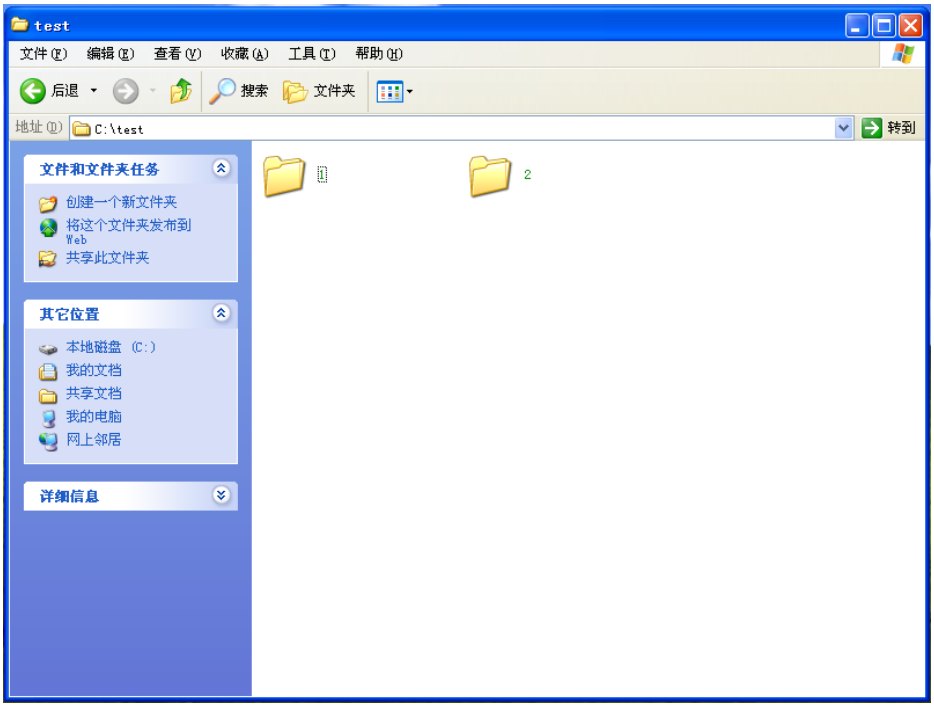
（11）输入在步骤（9）中为保护私钥设置的密码，选择将证书放入“个人”存储区中，单击“下一步”按钮，完成证书导入，见图三十五。



图三十五 证书的导入

（12）再次双击加密文件击中的文件，记录实验结果，并对其进行分析说明。

再次打开加密的文件，发现可以可以访问，文件名称字体问绿色表示是加密的文件。这是因为用户 MYCOMPUTER 获得了管理员用户的证书，再进行身份认证的时候，系统便会认为该用户得到了管理员的授权，所以给予访问权限（图三十六）。



图三十六 再次访问结果

任务六　利用 MBSA 检查和配置系统安全

MBSA 是微软公司提供的安全审计工具，可以从微软免费下载，其安装过程也非常简单，按照提示一步步安装即可。下面对 MBSA 的使用方法进行介绍。

（MBSA 下载地址：http://www.microsoft.com/en-us/download/details.aspx?id=7558）

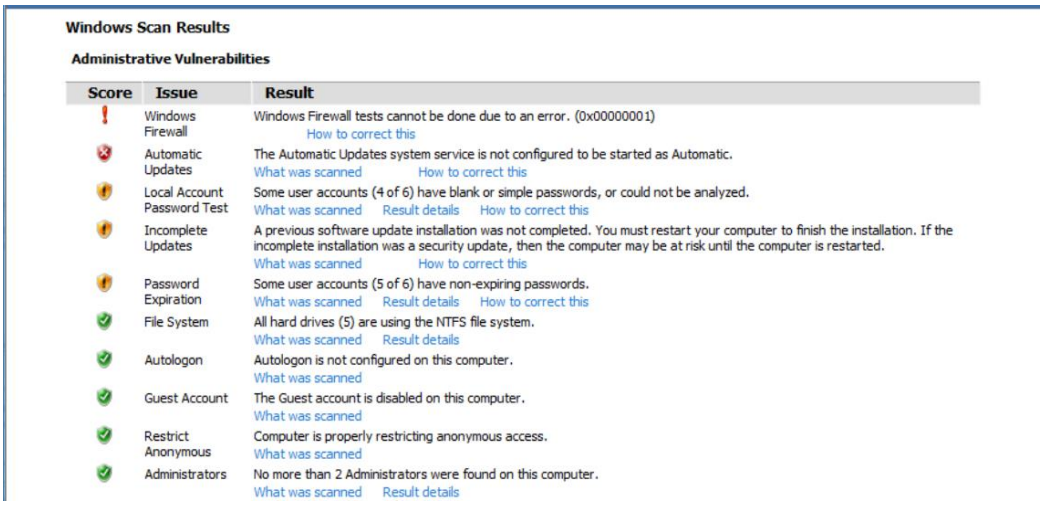
1. 检查系统漏洞

（1）双击打开 MBSA，在弹出的窗口中选择 Scan a computer。

（2）在弹出的窗口中填写本地计算机名称或者 IP 地址，并选择希望扫描的漏洞类型。这里采用全部漏洞扫描，单击“start scan”按钮，扫描计算机。

注意：由于扫描过程中需要连接 Microsoft 网站，因此需要事先配置好网络。

（3）扫描完成后，在实验报告中记录扫描结果，见图三十七。



图三十七 扫描结果

2. 查看安全性报告并手动修复漏洞

安全性报告中，最左侧一览为评估报告，其中红色和黄色的叉号表示该项目未能通过测试；雪花图标表示该项目还可以进行优化，也可能是程序跳过了其中的某项设置。感叹号表示尚有更详细的信息；绿色的对勾表示该项目已通过测试； What was scan 表明检查的项目，result scan 中详细的说明了该项目中出现的问题， how to correct this 说明了解决的方式。

（1）首先查看报告中评估结果为叉号的项目（这里选择 file system）,打开 result detail，查看该项检查中出现的具体问题（图三十八）。

Additional System Information

Score	Issue	Result
	Auditing	Neither Logon Success nor Logon Failure auditing are enabled. Enable auditing and turn on auditing for specific events such as logon and logoff. Be sure to monitor your event log to watch for unauthorized access. What was scanned How to correct this
	Services	No potentially unnecessary services were found. What was scanned
	Shares	6 share(s) are present on your computer. What was scanned Result details How to correct this
	Windows Version	Computer is running Microsoft Windows Unknown. What was scanned

Internet Information Services (IIS) Scan Results

Score	Issue	Result
	IIS Status	IIS is not running on this computer.

SQL Server Scan Results

Instance MSSQL13E.LOCALDB

Administrative Vulnerabilities

Score	Issue	Result
	Registry Permissions	Internal error.(43.7) What was scanned How to correct this
	SQL Server/MSDE Security Mode	SQL Server and/or MSDE authentication mode is set to SQL Server and/or MSDE and Windows (Mixed Mode). What was scanned How to correct this
	Service Accounts	SQL Server, SQL Server Agent, MSDE and/or MSDE Agent service accounts are not members of the local Administrators group and do not run as LocalSystem. What was scanned
	CmdExec role	CmdExec is restricted to sysadmin only. What was scanned
	Folder Permissions	What was scanned Result details
	Sysadmins	[DBNETLIB][ConnectionOpen (Connect()).]SQL Server 不存在或拒绝访问。 What was scanned

图三十八 具体问题查看

（2）单击 how to correct this 按钮，弹出的窗口显示了有关如何修改项目设置的提示信息。根据提示，我们可以修改不符合安全性要求的设置。

测试记录分析结论

（测试记录见实验步骤）

实验思考题

（1）如何检查系统是否允许 guest 账户登陆？

① 右键单击“开始”按钮，打开“资源管理器”，选择“控制面板”中的“用户和密码”项；在弹出的对话框中列出了系统的所有账户，可以查看 guest 庄户的启用状态。

② 打开“控制面板”中的“管理工具”，选中“计算机管理”中“本地用户和组”，打开“用户”，查看 guest 账户启用状态。

（2）三种日志文件分别记录什么样的事件？

应用程序日志

	记录由应用程序产生的事件。例如，某个数据库程序可能设定为每次成功完成备份操作后都向应用程序日志发送事件记录信息。应用程序日志中记录的时间类型由应用程序的开发者决定，并提供相应的系统工具帮助用户使用应用程序日志。 **安全性日志** 记录与安全相关事件，包括成功和不成功的登录或退出、系统资源使用事件等。与系统日志和应用程序日志不同，安全日志只有系统管理员才可以访问。 **系统日志** 记录由 Windows XP/2000 操作系统组件产生的事件，主要包括驱动程序、系统组件和应用软件的崩溃以及数据丢失错误等。系统日志中记录的时间类型由 Windows XP/2000 操作系统预先定义。 （3）如何查看 MBSA 扫描安全性报告？ 安全性报告中，最左侧一览为评估报告，其中红色和黄色的叉号表示该项目未能通过测试；雪花图标表示该项目还可以进行优化，也可能是程序跳过了其中的某项设置。感叹号表示尚有更详细的信息；绿色的对勾表示该项目已通过测试； What was scan 表明检查的项目，result scan 中详细的说明了该项目中出现的问题， how to correct this 说明了解决的方式。
小　结	通过实验本次实验，基本掌握掌握 Windows 账户与密码的安全设置、文件系统的保护和加密、安全策略与安全模板的使用以及审核和日志的启用、本机漏洞检测软件 MBSA 的使用等， 并且了解到 Windows XP 系统在用户管理上十分安全并且其使用 NTFS 文件系统，通过设置文件夹的安全选项来限制用户对文件夹的访问。 同时，通过本次实验学习 MBSA 工具的安装及使用，并学会利用 MBSA 工具检查和配置系统安全，通过分析安全报告，了解当前系统的安全等级。 **参考文献** [1]quers.XP 系统文件夹没有安全选项卡怎么处理？ [EB/OL].http://www.xitongzhijia.net/xtjc/20170504/96996.html,2017-05-04. [2]百度百科.计算机系统日志 [EB/OL].https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%B3%BB%E7%BB%9F%E6%97%A5%E5%BF%97/3536294?fr=aladdin,2019-11-8.
以下由实验教师填写	

记　事 评　议	
成绩评定	平时成绩_____　　实验报告成绩_____　　综合成绩 _____ 指导教师签名：