实验三 Windows 安全机制

2024 年 3 月 13 日

一、实验目的

1. 了解 Windows 密码策略和锁定策略的主要内容和用途，掌握 Windows 安全策略配置方法。

2. 了解 Windows 审核策略的主要内容和用途，掌握 Windows 审核策略的配置方法。

3. 理解 EFS 文件加密原理，掌握 EFS 文件加密方法。

二、实验环境

Windows 7 操作系统（如果不使用机房电脑，需要自行安装 Win7 虚拟机）

三、Windows 安全配置基本要求

我国信息系统等级保护标准对主机安全和应用安全提出了明确的要求，包括身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、资源控制等方面。根据等级保护标准要求，对 Windows 安全配置要求主要分为以下 6 类。

1. 账户配置要求

账户配置要求是针对用户账户信息保护提出的安全配置要求，主要用于加强对用户账户信息的管理，防止攻击者暴力猜测用户口令或者非法窃取账户信息。主要包括锁定阈值、账户锁定时间和复位账户锁定计数器三个配置项。

2. 口令配置要求

口令配置要求是针对用户口令的长度、复杂度及使用期限等提出安全配置要求，防止口令设置过于简单导致的非法入侵事件。

3. 用户权限配置要求

用户权限配置要求是针对本机用户及用户组对系统资源的访问权限提出的安全配置要求，包括远程访问、创建和访问文件对象、加载设备驱动、执行系统任务等。

4. 审核和日志配置要求

审核和日志配置要求是针对系统日志中所记录的事件和审计方式提出的安全配置要求，可以通过配置加强日志审计，详细记录系统操作，以便通过日志对安全事件进行溯源。

5. 安全选项配置要求

安全选项配置要求是针对操作系统组策略编辑器中的安全选项策略提出的安全配置要求，包括用户账户控制、Microsoft 网络服务器、关机、恢复控制台、交互式登录、设备、网络安全等方面的要求。

6. 组件配置要求

组件配置要求是针对用户安装的操作系统组件提出的安全配置要求。主要包括 IE 管理器、附件管理、电源管理、显示管理、会话服务、系统服务和网络服务等方面的配置要求。

四、实验内容

1. Windows 用户密码设置

（1）Win+r 键打开运行对话框，在对话框中输入 secpol.msc，打开 Windows 本地安全策略窗口， 如图 1.1 所示。

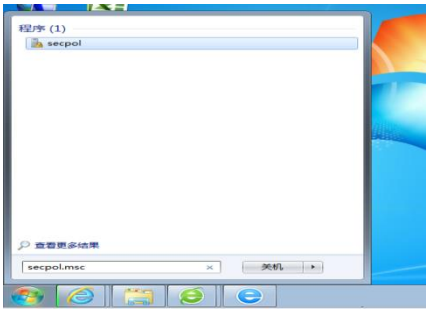

图 1.1 “运行”对话框

（2）在本地安全策略窗口中，展开左侧树形菜单“安全设置”—>“账户策略”，选择密码策略选项，在窗口右侧将会出现密码策略项。

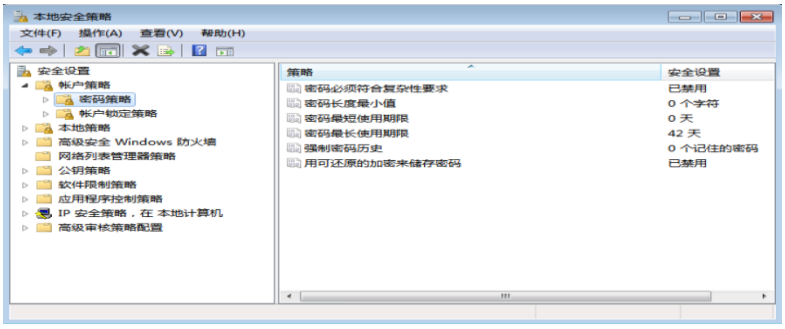

图 1.2 本地安全策略界面

（3）根据需要确定密码长度最小值、密码最长使用期限、密码最短使用期限、强制密码历史等的设置策略，例如设置如下表所示规则。双击对应的策略选项，在打开的对话框中进行设置。

策略	值	策略	值
密码复杂性要求	启用	密码最长留存期	15 天
密码长度最小值	6 位	强制密码历史	5 个

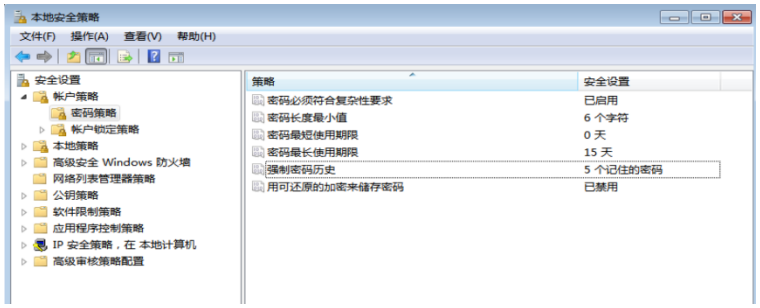

图 1.3 密码策略设置示例

（4）依次选择：“开始”—>“控制面板”—>“管理工具”—>“计算机管理”选项，展开界面左侧树形菜单“管理工具”—>“本地用户和组”，双击“用户”选项，在界面右侧列出系统中所有用户名称，在右侧空间中右击，选择“新用户”选项，新建立一个用户 test，密码为空。系统将弹出错误信息提示。为 test 设置用户设置密码 Aa123456，满足复杂性要求，密码设置成功。

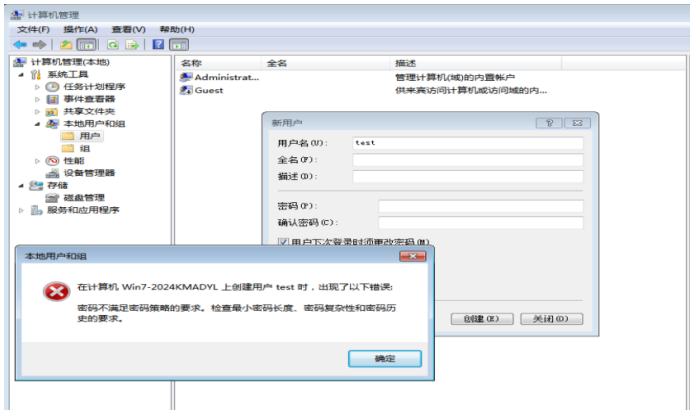

图 1.4 密码设置出错

2. 用户锁定策略设置

（1）在“本地安全策略”窗口中展开“安全设置”—>“账户策略”，选择“账户锁定策略”选项，在窗口右侧，出现账户锁定策略。如图 2.1 所示：

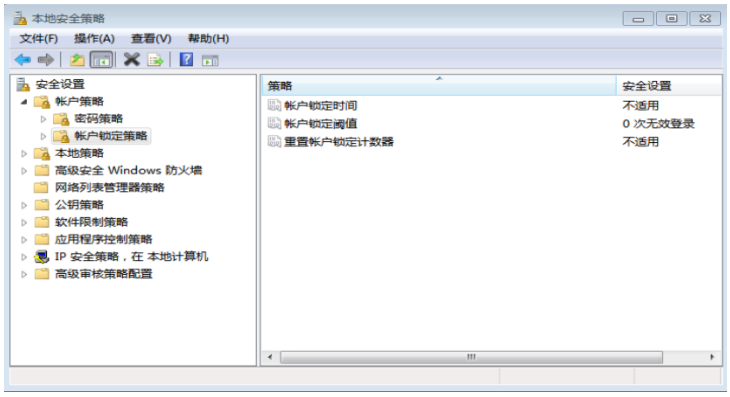

图 2.1 用户锁定策略设置窗口

（2）根据需要设置锁定策略，例如可以设置如图 2.2 所示的锁定策略。

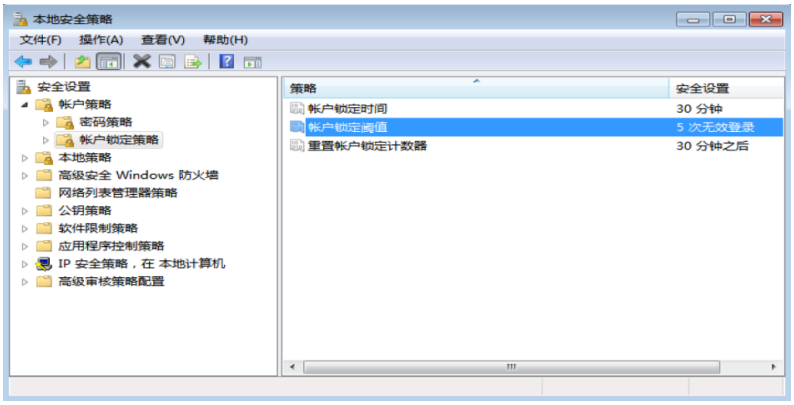

图 2.2 账户锁定策略设置示例

（3）通过测试案例验证锁定策略。以前面创建的 test 用户身份登录，连续输错 5 次密码后，用户登录界面将被锁定。等待 1 分钟后，锁定取消，输入正确密码，可以登录系统。

3. Windows 审核策略配置

3.1 文件操作的审计

（1）打开“本地安全策略”对话框，选择“本地策略”—>“审核策略”，双击“审核对象访问”，勾选“成功”和“失败”，如图 3.1.1 和图 3.1.2 所示：

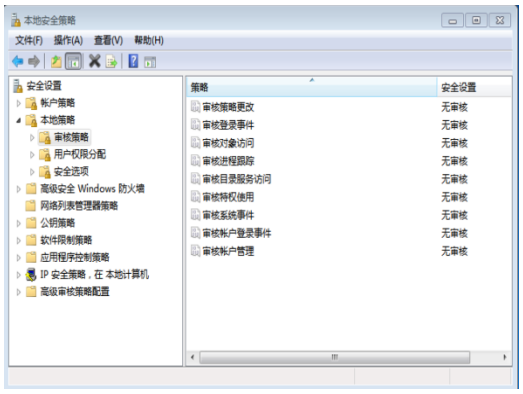

图 3.1.1 审核策略设置窗口

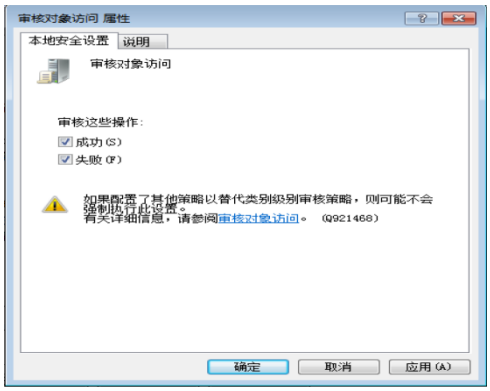

图 3.1.2 设置审核对象访问策略

（2）在硬盘上新建一个名为“123.txt”的文件，右击该文件，在弹出的快捷菜单中选择“属性”选项，然后单击“安全”选项卡，如图 3.1.3 所示：

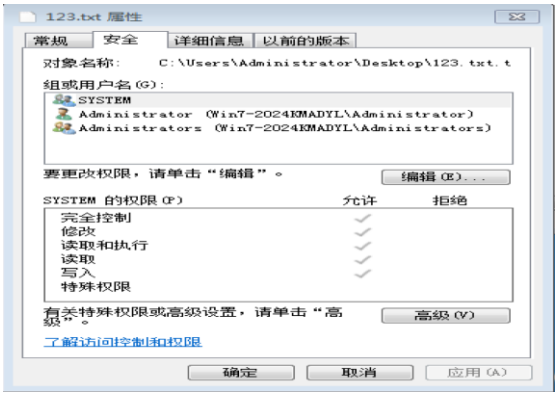

图 3.1.3 安全属性设置窗口

（2）单击图 3.1.3 中的“高级”按钮，然后选择“审核”选项卡，出现如图 3.1.4 所示的对话框，单击“编辑”按钮，出现如图 3.1.5 所示的窗口。

图 3.1.4 文件审核界面

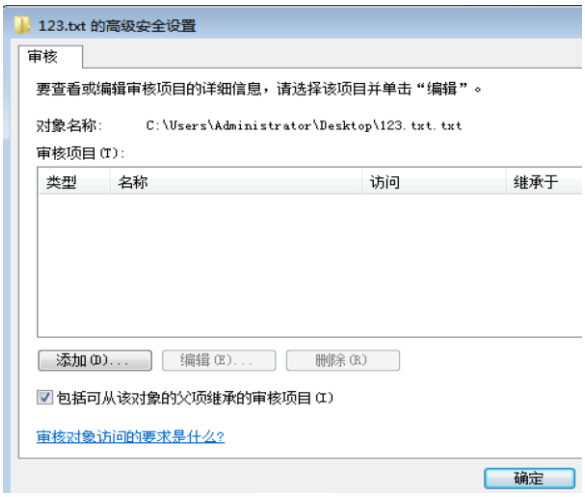

图 3.1.5 文件审核项目编辑界面

（3）在图 3.1.5 中单击“添加”按钮，出现如图 3.1.6 所示的“选择用户或组”对话框，在“输入要选择的兑现名称”编辑框中输入“Everyone”。单击“确定按钮”，出现如图 3.1.7 所示的“123.txt”的审核项目对话框，在访问列表中选择“删除”和“更改权限”的功能，设置完成后单击“确定”按钮。至此，对“123.txt”的审计项设置完成，如图 3.18 所示。

图 3.1.6“选择用户或组”对话框

图 3.1.7“123.txt 的审核项目”对话框

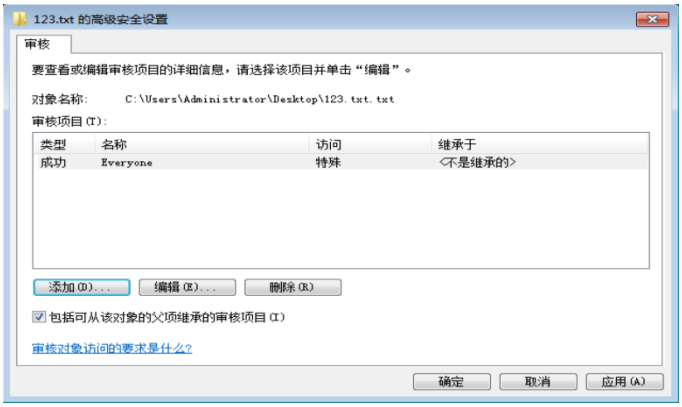

图 3.1.8 文件审核设置完成

（4）为验证审核策略是否起作用，查看删除文件的操作是否被记录到日志中。依次选择“开始”—>“控制面板”—>“管理工具”—>“事件查看器”—>“Windows 日志”—>“安全性”选项，出现如图 3.1.9 所示窗口，可以看到系统成功审核了文件删除的事件。

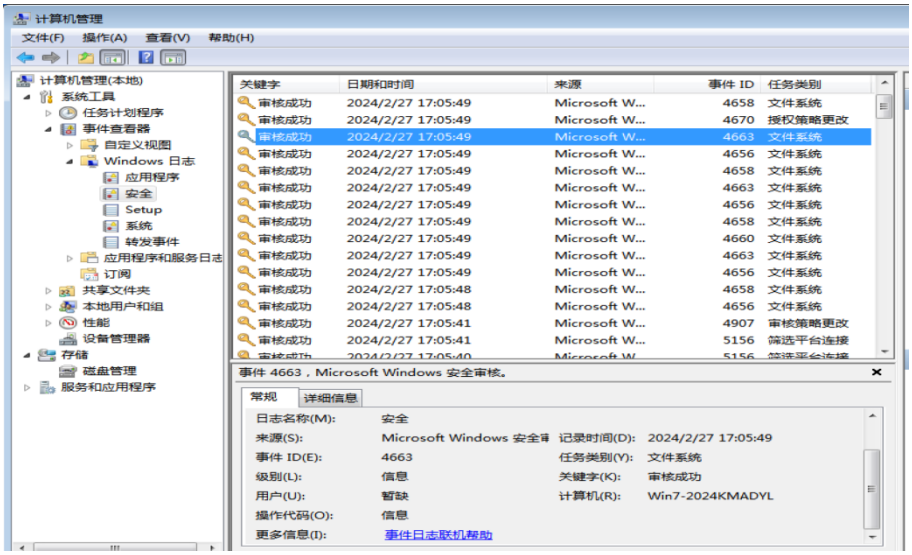

图 3.1.9 文件审核项设置完成

3.2 Windows 账户管理操作的审计

（1）打开“本地安全设置”对话框，选择“本地策略”—>“审核策略”选项，双击“审核账户管理”选项，勾选“成功”和“失败”，如图 3.2.1 所示。

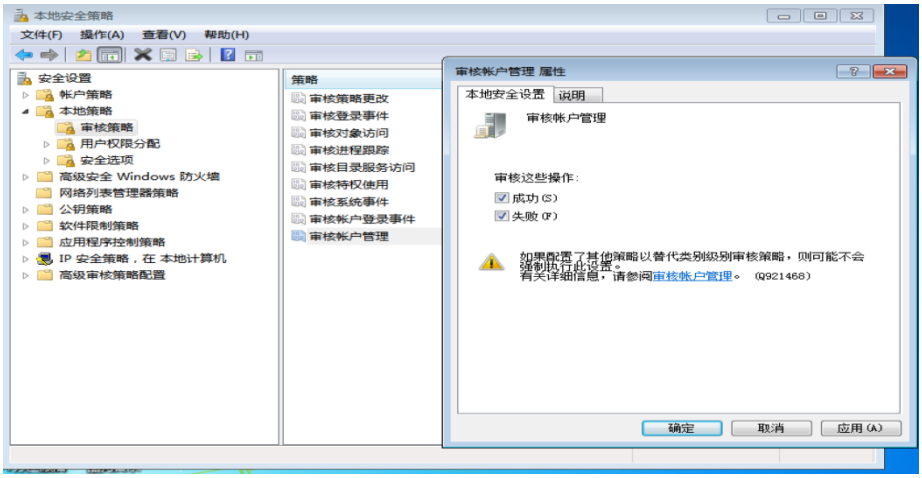

图 3.2.1 用户管理审核设置

（2）为验证审核策略是否起作用，在系统中添加一个账户，查看日志中是否记录新建账户的事件。

3.3 Windows 用户登录事件的审计

（1）打开“本地安全设置”对话框，选择“本地策略”—>“审核策略”选项，双击“审核账户登录事件”选项，勾选“成功”和“失败”。

（2）**为验证上述审核策略是否起作用，注销当前用户，并重新登录，查看系统是否记录了该事件。**

4 EFS 数据加密

（1）在 D 盘中创建文件夹 test(如果是 Win7 虚拟机，则在 C:\Users\Public\ 中创建文件夹 test)，在该文件夹下创建文件 test.txt,在文件中写入内容“This is a testing file!”，保存后关闭文件。右击文件，打开“属性”窗口，选择“常规”选择，单击“高级”按钮，选择“加密内容以便保护数据”，单击“确定”按钮，如图 4.1 所示。

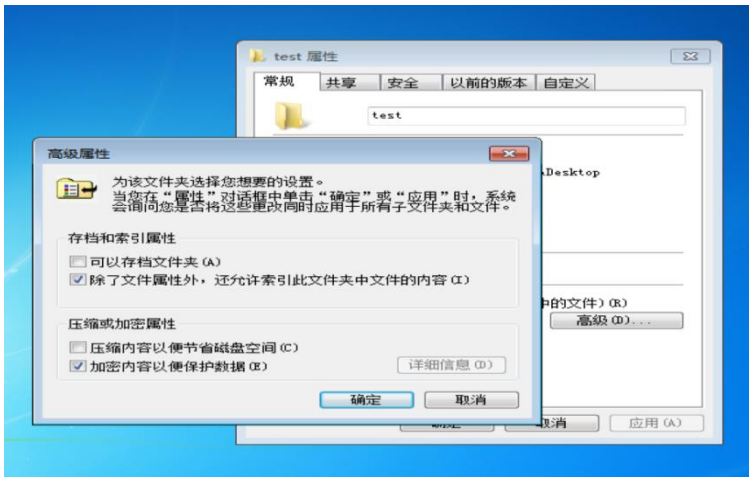

图 4.1 文件加密

（2）打开计算机管理窗口，展开界面左侧的“计算机管理”->“本地用户和组”，双击“用户”选项，在界面右侧将会列出系统重所有用户名称，在右侧空白处右击，在弹出的快捷菜单中选择“新用户”选项，创建一个名位 USER 的新用户，且不要创建为计算机管理员用户，如图 4.2 所示。

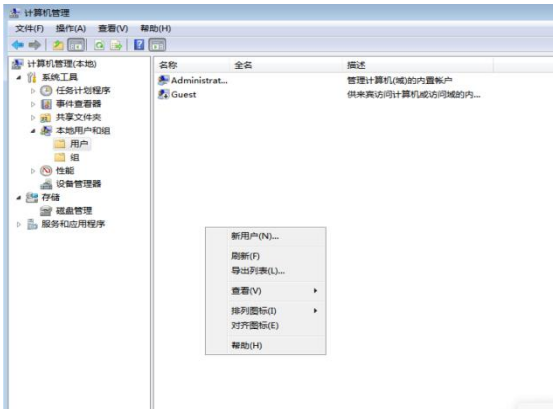

图 4.2 新建用户

（3）以刚刚新建的 USER 身份登录系统，导航到“D:\test”(“C:\Users\Public\test”)，双击“test.txt”，发现无法打开该文件，说明文件已经加密，如图 4.3 所示。

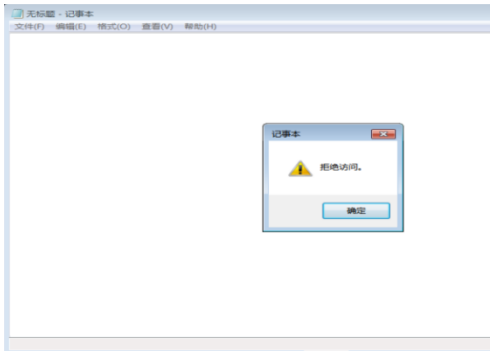

图 4.3 打开加密文件失败

（4）再次切换用户，以加密文件的账户登录系统，单击“开始”按钮，在“运行”框中输入mmc，打开系统控制台，单击左上角的“文件”菜单，选择“添加/删除管理单元”子菜单，如图 4.4 所示。在弹出的对话框左侧的可用管理单元中选择“证书”，如图 4.5 所示，单击“添加”按钮。在弹出的“证书管理”对话框中选择“我的用户账户”，然后单击“完成”按钮，如图 4.6 所示。

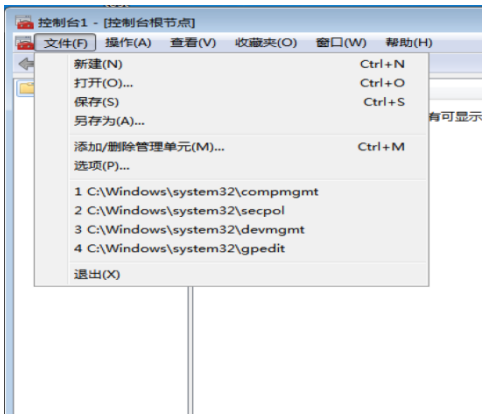

图 4.4 系统控制台窗口

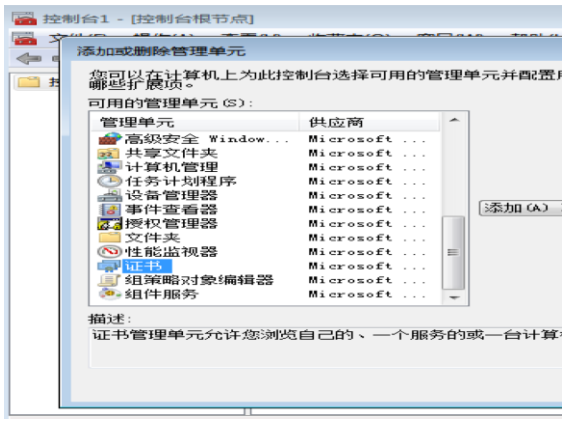

图 4.5 “添加或删除管理单元”对话框

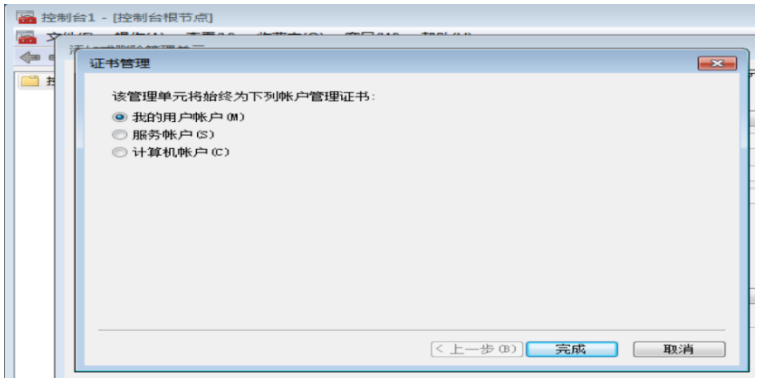

图 4.6 “证书管理”对话框

（5）在控制台窗口左侧的目录中选择“证书”—>“个人”—>“证书”选项，如图 4.7 所示。选中证书，右击，在弹出的快捷菜单中选择“所有任务”—>“导出”，打开“证书导出向导”对话框，如图 4.8 所示。在图 4.8 中单击“下一步”按钮，在出现的如图 4.9 所示对话框中选择“是，导出私钥”，然后继续单击“下一步”，出现如图 4.10 所示的对话框，设置保护私钥的密码。单击“下一步”按钮，出现如图 4.11 所示的对话框，设置要导出的文件的文件名，并设置要导出文件的保存路径，**注意一定要保存在 C 盘**，完成证书导出。

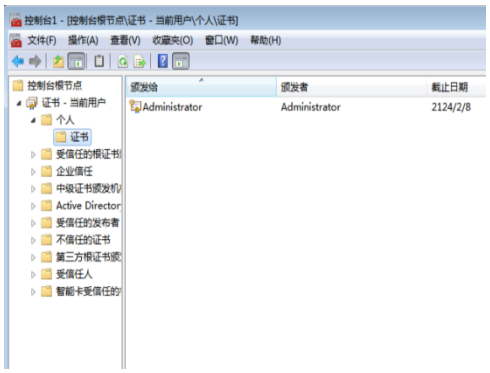

图 4.7 个人证书管理

图 4.8“导出证书向导”对话框

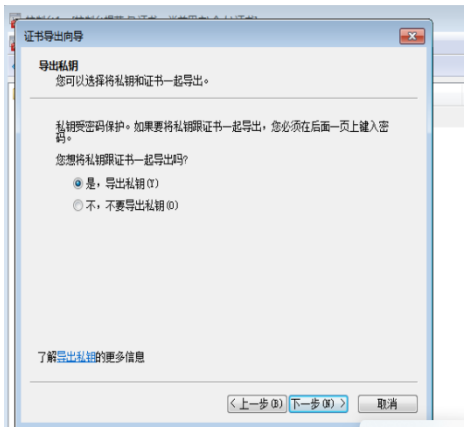

图 4.9 导出私钥

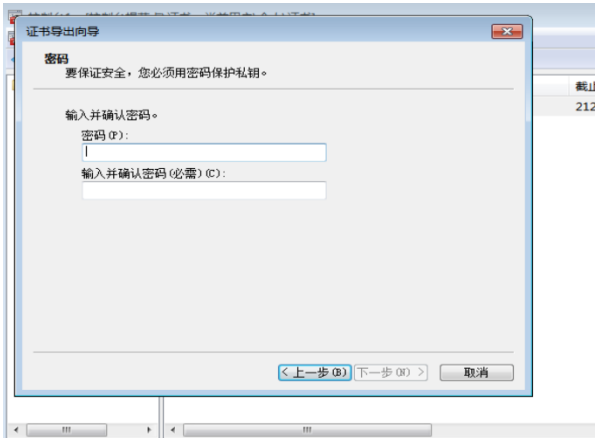

图 4.10 为私钥设置密码保护

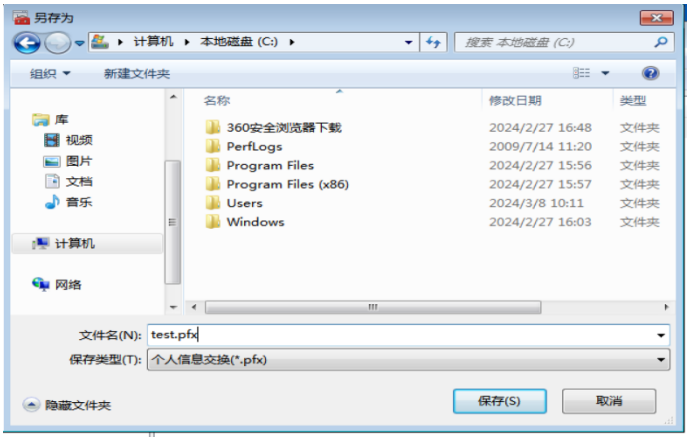

图 4.11 指定导出文件名

（6）切换用户，以新建的 USER 用户身份登录，按刚才的步骤打开控制台并添加证书，然后选中个人，会发现右边没有证书。选择“个人”选项，选择“所有任务”—>“导入”选项，如图 4.12 所示，在图 4.13 所示的对话框中，选择要导入的证书文件，输入之前设置的私钥保护密码，完成证书导入。

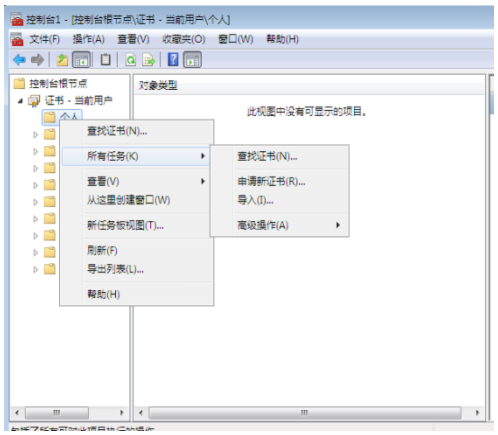

图 4.12 导入证书

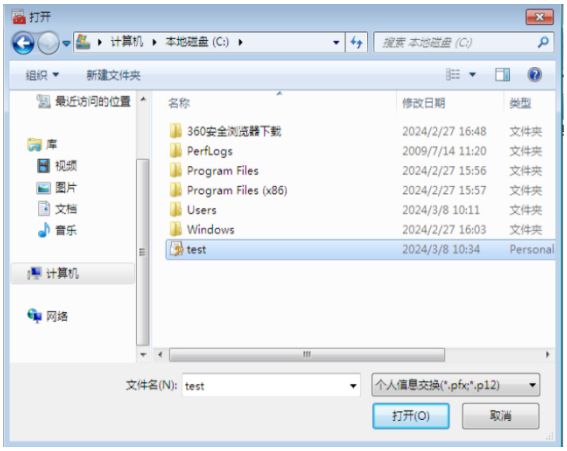

图 4.13 指定要导入的证书文件

（7）导入完成后可以在控制台的“个人”栏看见原来没有证书的地方现在已经有了一个新的证书，如图 4.14 所示。

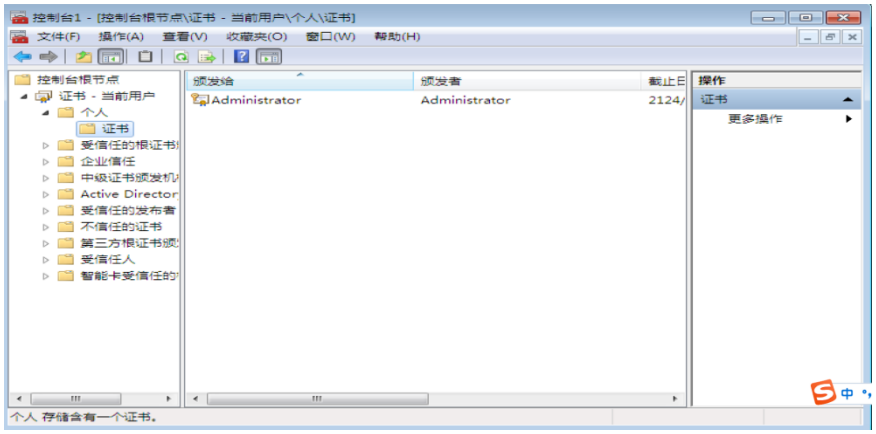

图 4.14 成功导入证书

（8）再次进入 C 盘，双击加密文件夹中的文件，测试文件是否能正常打开？

5 除了 EFS 文件加密机制，Windows Vista 之后的版本还提供了 BitLocker 加密机制，请比较这两种加密机制的不同及适用场景。

6 利用 Windows 安全策略使得用户登录窗口不出现上次登录的用户名信息。

五、提交：实验报告（ pdf，内含关键步骤和结果的截图）。报告命名格式：学号-姓名-实验 4.pdf 发送到 yanlin@jnu.edu.cn 。截止日期：2024 年 3 月 20 日 14:00。