

信息与软件工程学院上机实验报告

(第 3 次)

一、实验名称

实验三：操作系统安全加固实验

二、实验目的及要求

1. 实验目的

通过本次实验，掌握 Windows 操作系统中账户与口令的安全设置、文件加密与证书授权、审核与日志启用、安全策略与安全模板应用等基本方法，建立一个较为完整的操作系统安全加固框架。

2. 实验要求

对 Windows 操作系统完成如下安全设置：

内容一：账户和口令的安全设置

通过账户口令的安全设置，有效地减少黑客攻击的成功率。一般电脑都使用 Windows 默认的账户口令，通过修改，可以提高电脑的安全性能。

内容二：用加密软件 EPS 加密硬盘数据

磁盘数据也是被攻击的对象。NTFS 格式的文件是一种安全文件系统，通过设置文件夹的权限，可以限制其他用户的访问，从而保障数据的安全性。使用数据加密软件，可以加强数据的安全性，并减少计算机、磁盘被窃或者被拆后数据失窃的隐患。加密后还可以控制特定用户对数据进行解密。

内容三：启用审核与日志查看

运用 Windows 系统中的审核与日志功能，可以进行入侵检测。面对系统攻击时，相关操作会被记录进日志，以便察觉和防御。

内容四：启用安全策略与安全模板

使用 Windows 安全模板，以便根据需求对各项安全属性进行简单配置。

三、实验环境

1. 实验平台：VMware Workstation Pro 25H2
2. 操作系统：Windows 7 64-bit SP1
3. 系统工具：控制面板、本地安全策略、事件查看器、MMC 控制台
4. 文件系统：NTFS

四、实验设计

1. 调试过程及实验结果

1.1 账户和口令的安全设置

(1) 禁用 Guest 账户

首先对 Guest 账户进行处理。进入“我的电脑”中的“管理”，打开“系统工具 / 本地用户和组 / 用户”，查看当前系统中的用户列表。此时可以看到 Guest 账户仍然存在，说明默认来宾账户尚未被限制。



图 1: 本地用户和组中的用户列表

随后右键单击 Guest 账户，打开其属性窗口，在“账户已停用”前打勾并保存设置。该设置会关闭默认来宾账户的登录入口，减少系统被匿名或低权限方式尝试访问的可能性。

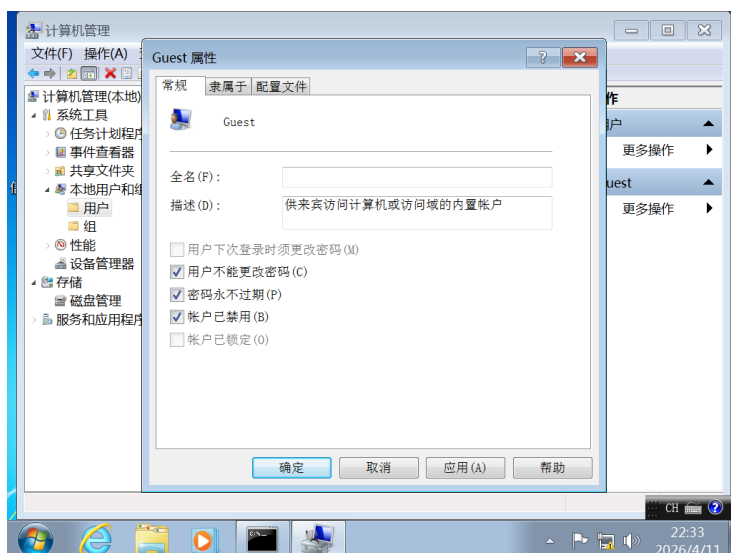


图 2: Guest 账户属性设置界面

设置完成后，返回用户列表可以看到 Guest 账户图标上出现了向下箭头，说明该账户已经被禁用。账户禁用后，默认账户可被直接尝试登录的机会会相应减少。



图 3: Guest 账户被禁用后的状态

(2) 启用账户策略

完成默认账户处理后，下一步是加强账户口令策略。打开“控制面板 / 管理工具 / 本地安全策略”，在“账户策略”下进入“密码策略”。这一部分用于提高口令设置门槛，降低弱口令、短口令和长期不更换口令带来的风险。

首先启用“密码必须符合复杂性要求”。启用这一项后，系统会要求用户设置

的口令包含多种字符类型，避免口令过于简单，从而提高口令被猜测或爆破的难度。

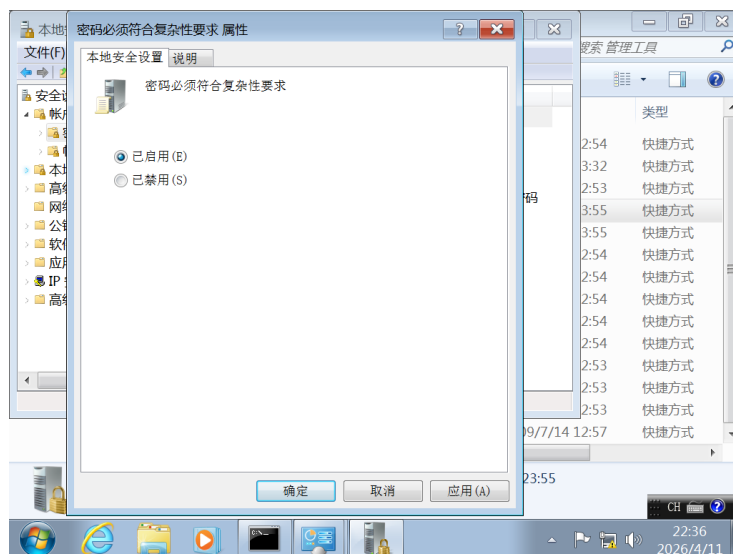


图 4: 启用“密码必须符合复杂性要求”

接着将“密码长度最小值”设置为 8。较短的口令往往更容易被枚举和试探，适当提高最小长度，是最直接、最有效的口令强化方式之一。

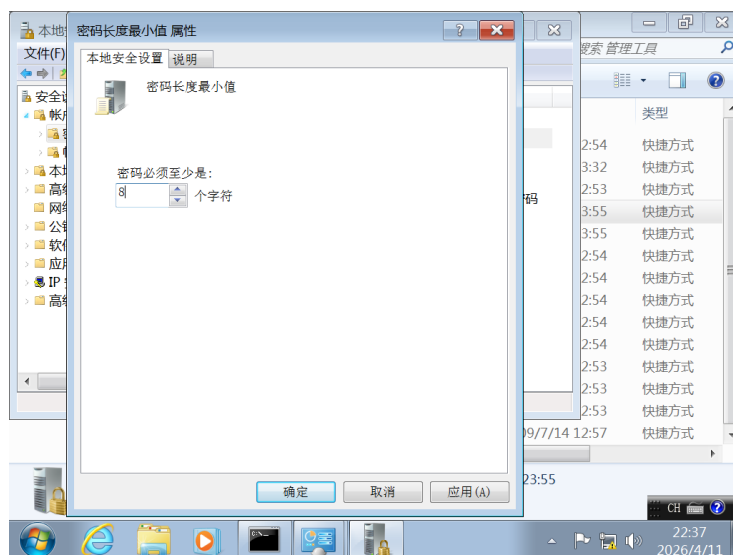


图 5: 设置密码最小长度为 8

随后把“密码最长使用期限”设置为 7 天。设置较短的使用期限后，账户口令需要按周期更换，从而减少同一口令长期使用的情况。

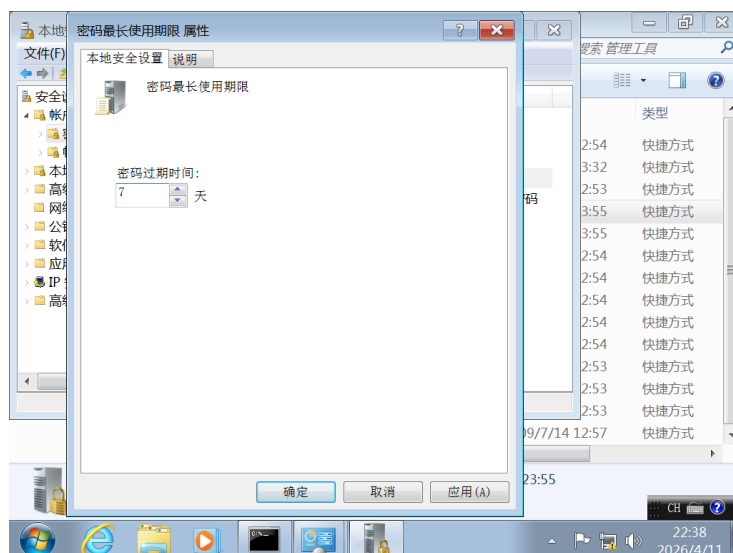


图 6: 设置密码最长使用期限为 7 天

在此基础上，继续调整“强制密码历史”，将其设置为不保留密码历史。虽然真实系统中通常会保留一定数量的历史口令以防重复使用，但这里主要记录实验中的实际设置结果。

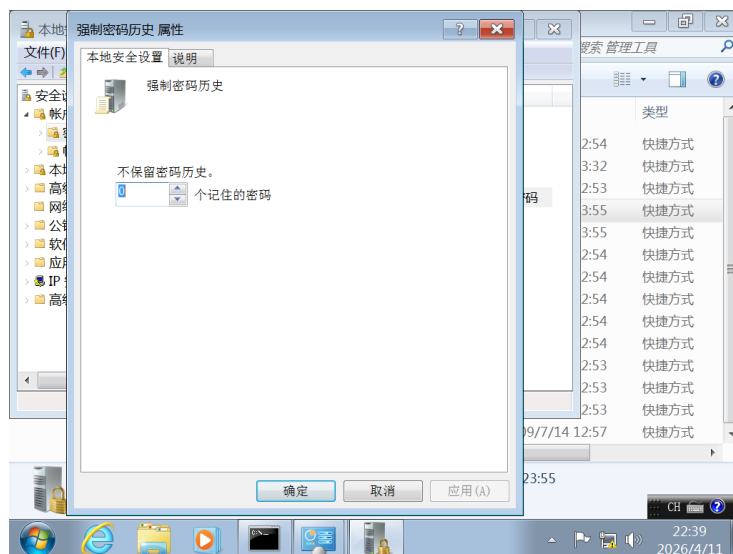


图 7: 设置不保留密码历史

最后启用“可还原的加密存储密码”选项。该设置同样属于密码策略中的一项配置内容。

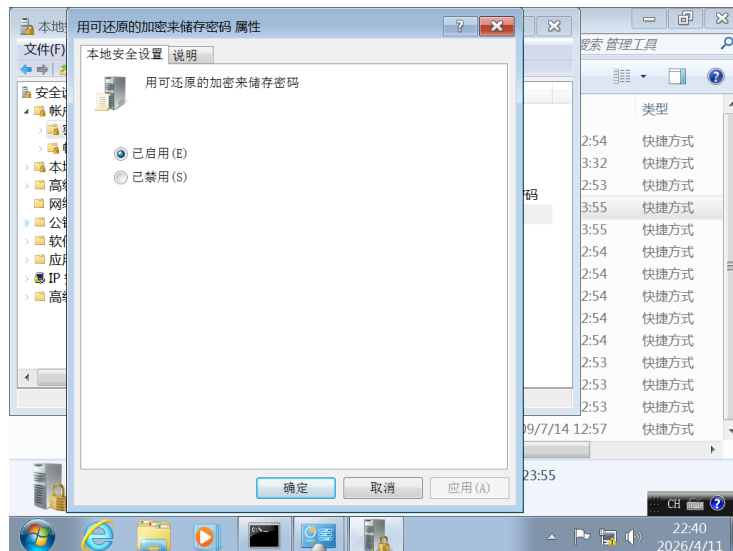


图 8: 启用可还原加密存储密码

经过以上设置后，系统口令管理具备了明确的复杂度、长度和更新周期要求，账户口令不再保持默认配置状态。

(3) 设置登录时不显示上次登录用户名

接下来，在“本地策略 / 安全选项”中找到“交互式登录：不显示最后的用户名”，并将其设置为“已启用”。Windows 默认可能会在登录界面保留上次登录用户的信息，而这会直接向攻击者暴露一个可尝试的用户名。

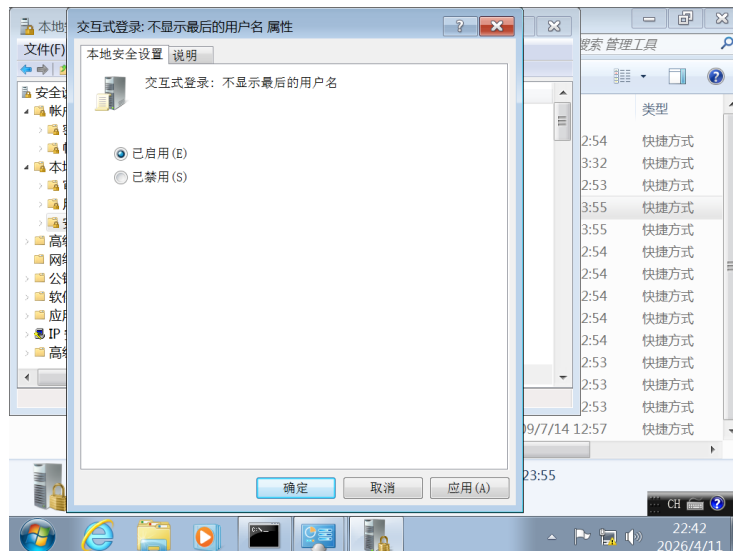


图 9: 启用“登录时不显示最后的用户名”

完成该设置后，系统登录界面将不会自动显示上一次登录的账户名，登录入口可直接暴露的用户信息随之减少。

(4) 禁止枚举账户名

账户和口令安全设置的最后一步，是禁止通过匿名方式枚举本地账户信息。继续在“本地安全策略”的“安全选项”中找到“不允许 SAM 账户和共享的匿名枚举”，并将其启用。

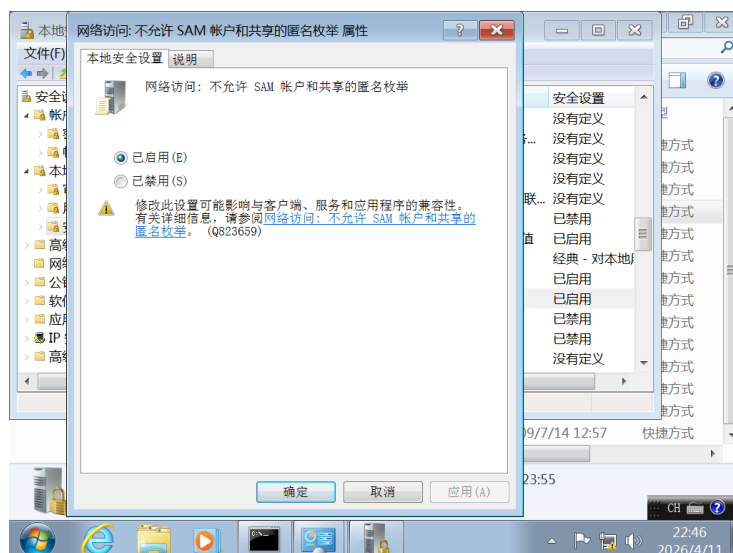


图 10: 启用“不允许 SAM 账户和共享的匿名枚举”

启用该策略后，远程匿名连接将更难获取本地账户和共享信息。这样做的效果，是减少攻击者在前期信息收集阶段可直接获取到的系统账户情报，从源头上压缩被动暴露面。

1.2 用加密软件 EPS 加密硬盘数据

(1) 文件加密设置

完成账户安全设置后，开始进行文件加密实验。在 NTFS 分区中选择测试文件，打开其属性窗口，在“高级”选项里勾选“加密内容以便保护数据”，从而对该文件启用 Windows 的文件加密机制。启用后，文件访问控制会与执行加密操作的账户证书关联。

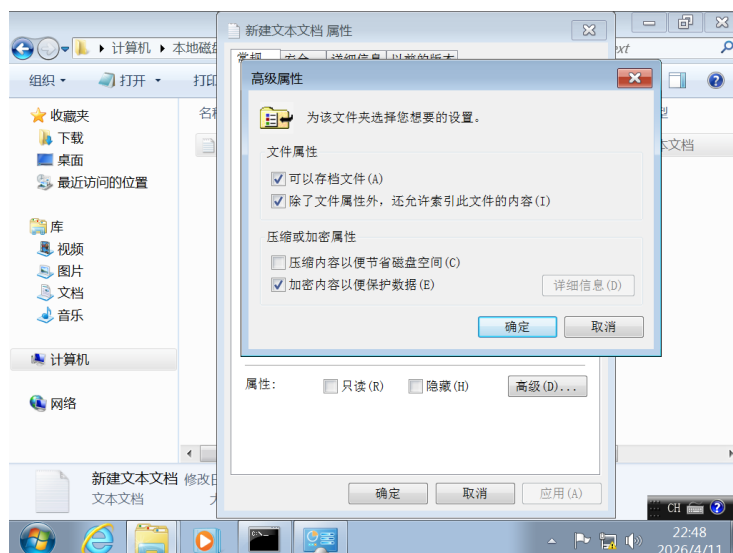


图 11: 对测试文档启用加密属性

(2) 创建测试用户

为了验证加密是否真正生效，又在控制面板中创建了一个名为“ ”的普通测试用户。该用户设置为受限账户，不具有管理员权限，便于观察非原始加密用户访问文件时的结果。



图 12: 创建名为“ ”的普通测试用户

(3) 验证加密有效性

创建完测试用户后，切换到用户“ ”登录系统，再次进入保存加密文件的位置，尝试直接打开之前已经加密的文档。结果显示，用户“ ”无法访问这个文件，文件权限已经与执行加密操作的账户证书绑定，其他本地用户登录后也不能直接读取。

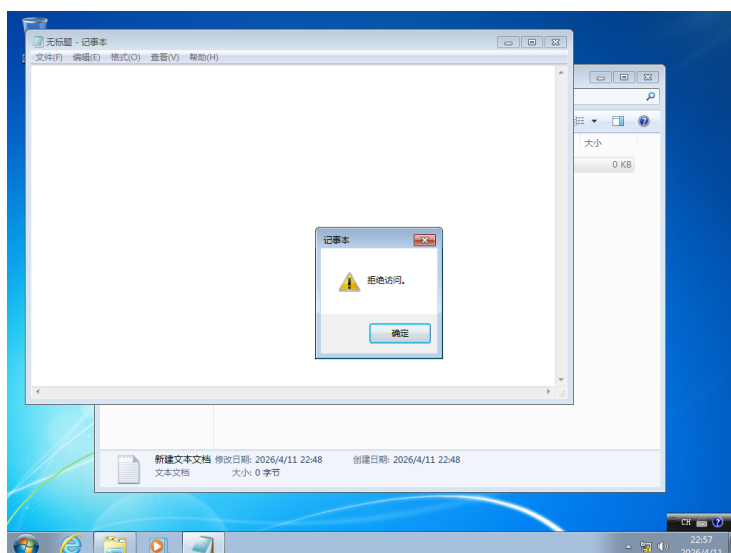


图 13: 用户“ ”无法访问加密文件

该结果说明，加密设置已经生效，未授权用户不能直接读取受保护文件。

(4) 证书导出与备份

为了让指定用户也能够访问该加密文件，切换回原来执行加密操作的用户，并通过‘mmc’打开控制台，添加“证书”管理单元，查看执行加密操作账户“个人”存储中的证书。这里可以看到与加密文件系统相关的个人证书，它是后续授权访问所需的凭据。

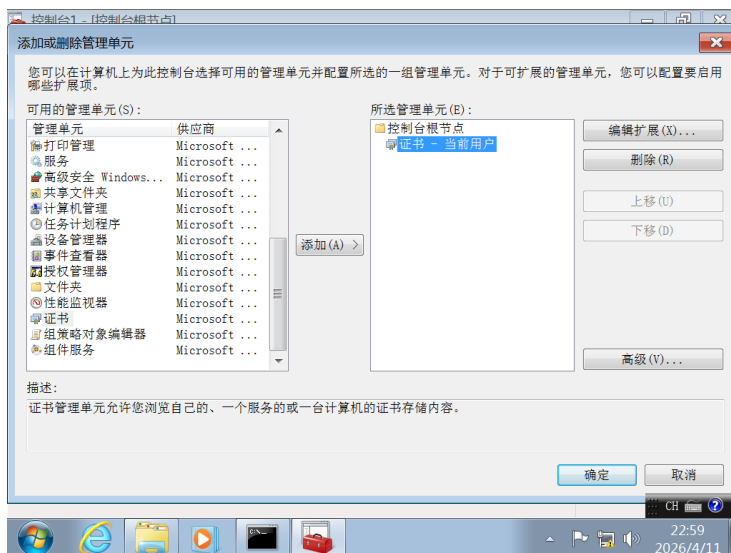


图 14: 查看执行加密操作账户的个人证书

接着启动证书导出向导，在导出过程中为私钥设置保护密码，密码设置为学号‘ ’。这样可以把原用户对加密文件的访问能力备份出来，

并限制其他人在不知道密码的情况下直接使用该证书文件。

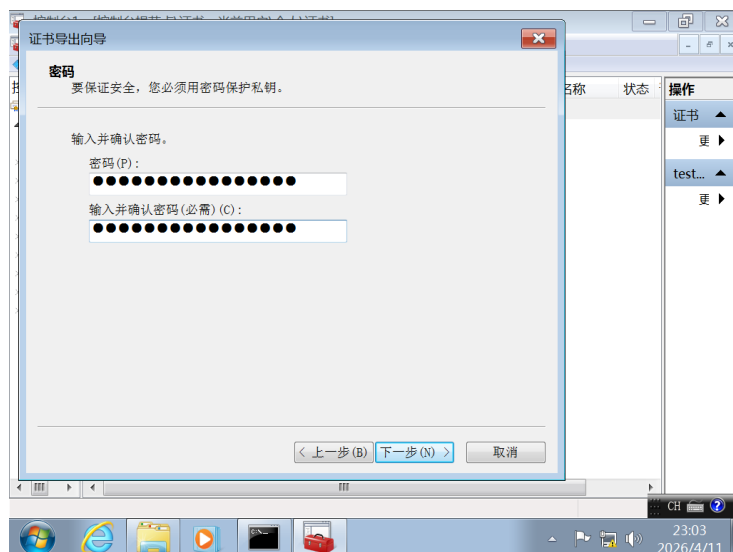


图 15: 导出证书时将私钥保护密码设置为学号

(5) 证书导入与授权

随后再次切换到用户“ ”，按相同方法打开 MMC 控制台并进入个人证书存储。此时可以看到该用户的“个人”证书列表原本是空的，用户“ ”尚未具备之前加密文件的解密能力。

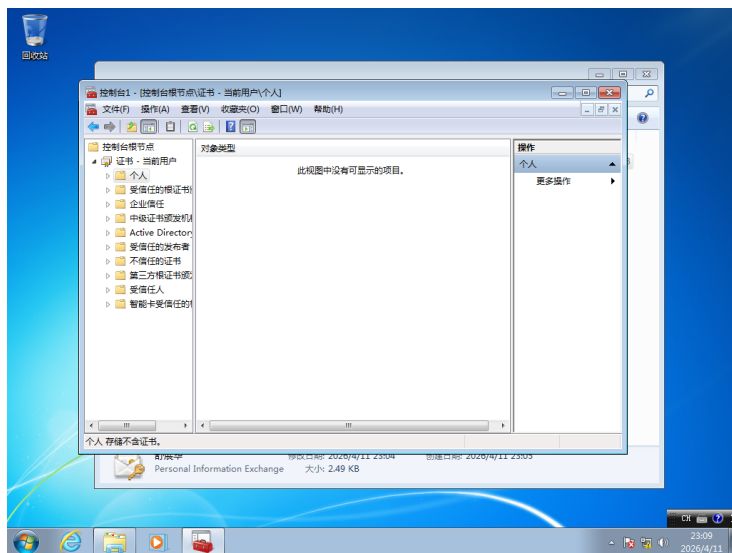


图 16: 用户“ ”导入前个人证书为空

然后执行证书导入操作，选择之前导出的证书文件，并输入导出时设置的学号密码‘ ’。只有密码正确，系统才会允许把带私钥的证书导入到用户“ ”的证书存储中，因此证书导入过程本身也受到密码限制。

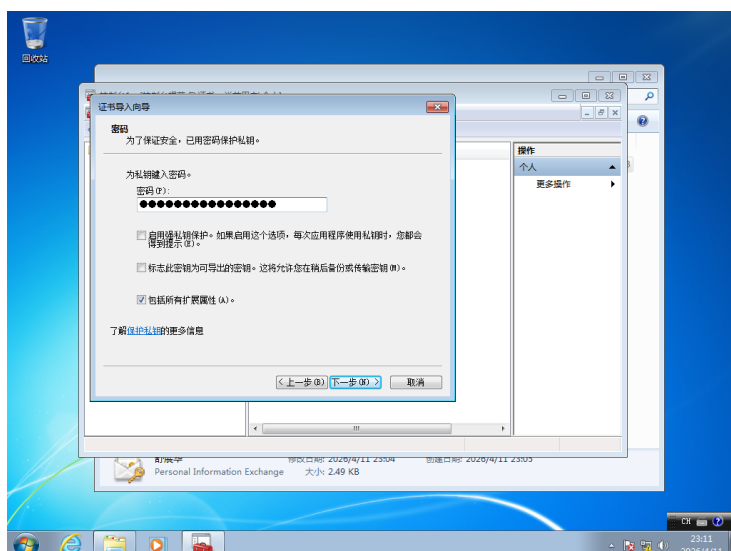


图 17: 导入证书时输入学号密码

导入完成后，用户“ ”的个人证书存储中已经能够看到对应证书，用户“ ”已经获得访问原加密文件所需的授权身份。

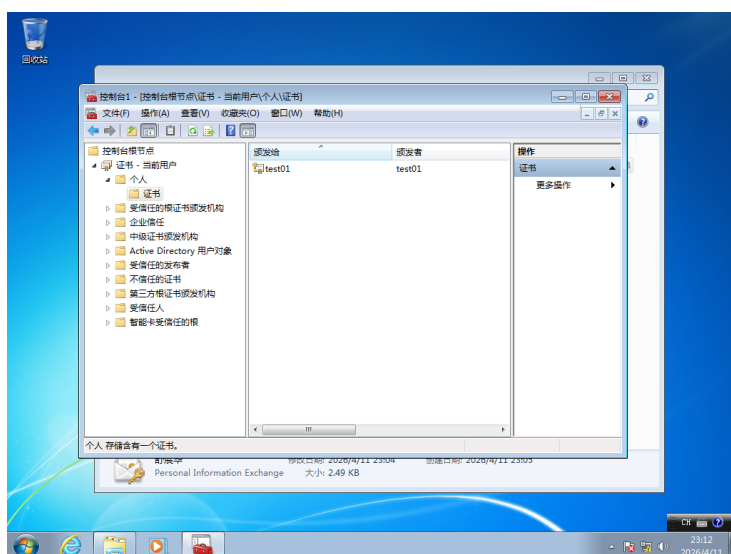


图 18: 用户“ ”成功导入个人证书

(6) 解密验证

最后再次使用用户“ ”访问之前的加密文件。此时文件可以被正常打开，说明授权已经生效，文件访问权限已经随证书转移到当前用户。

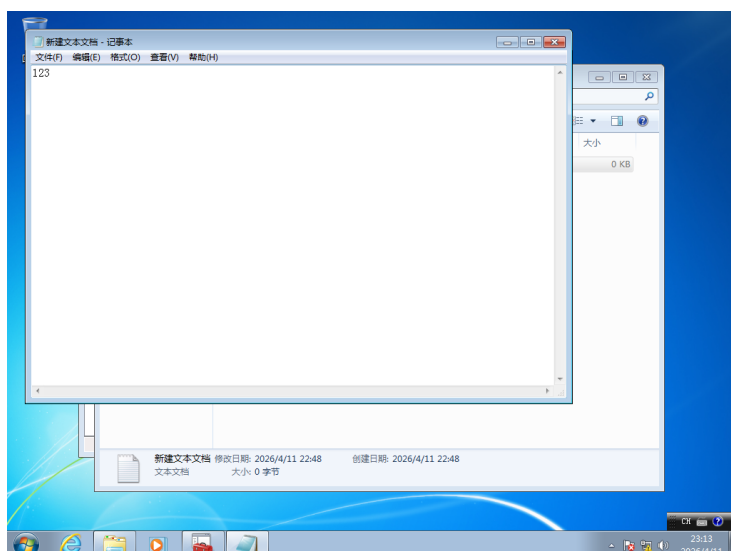


图 19: 导入证书后成功打开加密文件

这一部分实验的结果为：未授权时无法访问，导入正确证书后可以访问。
Windows 文件加密机制中的访问控制与证书授权在这里是一一对应的。

1.3 启用审核与日志查看

(1) 打开审核策略

完成文件保护后，继续启用审核功能。打开“控制面板 / 管理工具 / 本地安全设置”，进入“本地策略 / 审核策略”，找到“审核账户管理”并勾选“成功”和“失败”。
设置完成后，系统会对账户管理相关事件记录成功和失败日志。

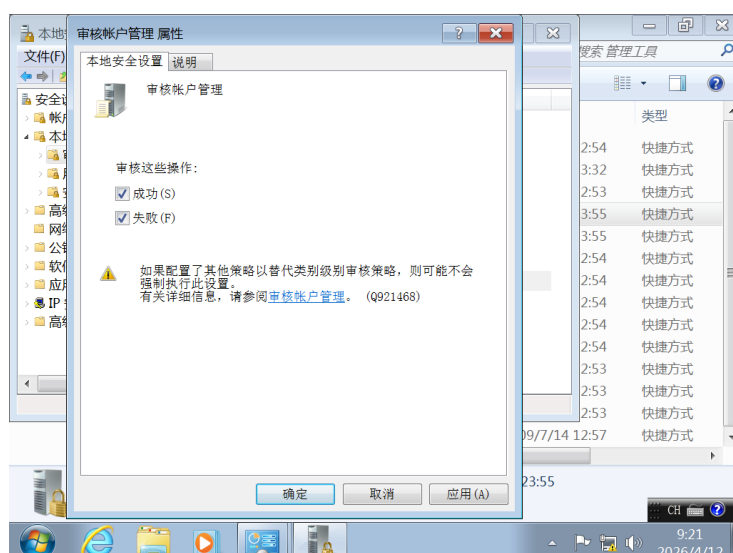


图 20: 修改“审核账户管理”的审核范围

启用审核策略之后，系统会把账户管理相关活动写入安全日志。

(2) 查看事件日志

在审核功能开启之后，打开“事件查看器”，进入“Windows 日志 / 安全”，查看系统已经记录下来的安全事件。这样可以直接验证前面的审核配置是否已经生效。

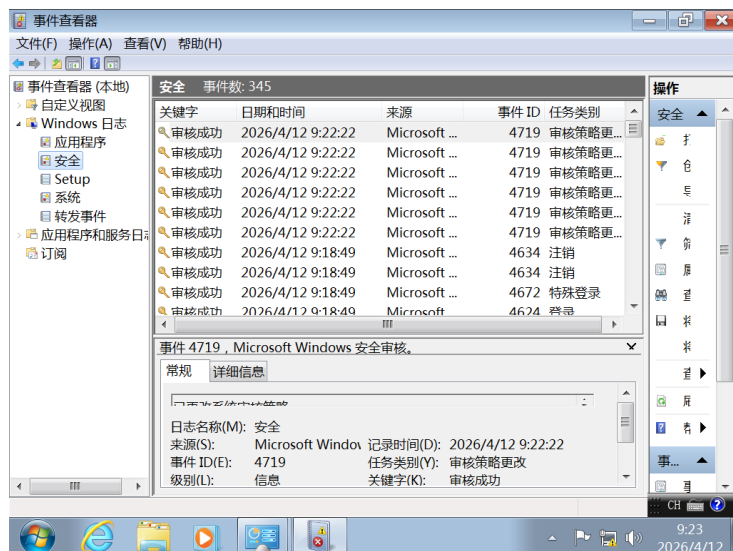


图 21: 在事件查看器中查看安全事件日志

从实验结果来看，安全日志中已经能够查看到相应记录，说明系统已经开始对相关安全事件进行审计记录。

1.4 启用安全策略与安全模板

(1) 创建安全模板

在完成前面几项单独配置之后，开始进行安全模板实验。先通过‘mmc’添加“安全模板”和“安全配置和分析”两个管理单元，然后在“安全模板”中创建一个新的自定义模板，并将模板名称填写为“”，描述填写为“自设模板”。这样做的目的是把零散的安全设置集中保存下来，方便后续统一分析和应用。

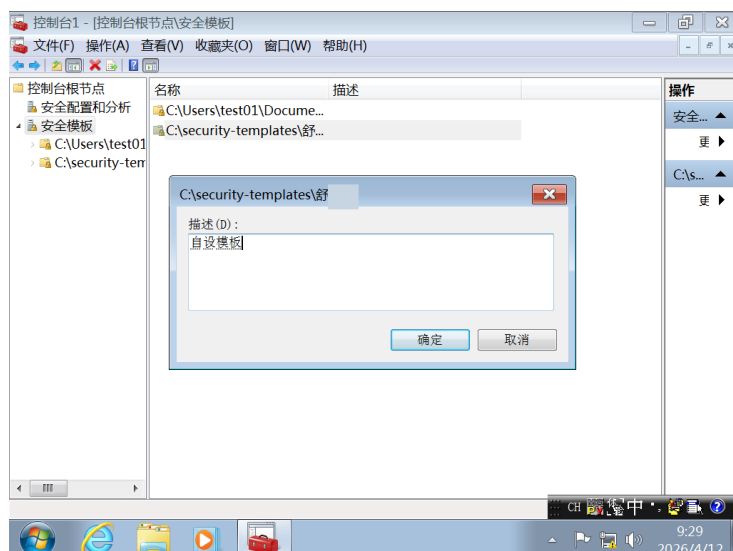


图 22: 创建名为“ ”的安全模板并填写描述

模板创建完成后，进入其中的“账户策略 / 密码策略”，先对“密码长度最小值”进行定义，并将其设置为 7。这样，安全模板中已经写入了具体的密码长度参数。

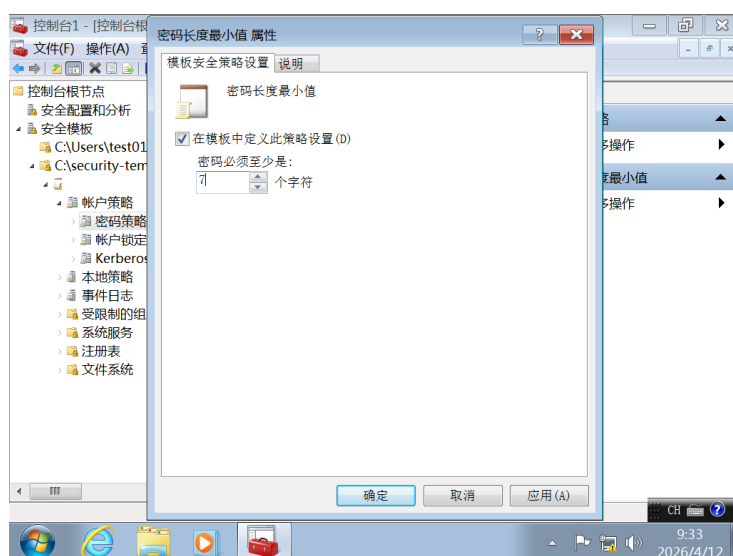


图 23: 在安全模板中设置密码长度最小值为 7

随后继续在模板中完善其他相关设置，直至完成整个自定义模板的配置。到这一步为止，一个可以被系统调用和分析的安全模板已经建立完成。

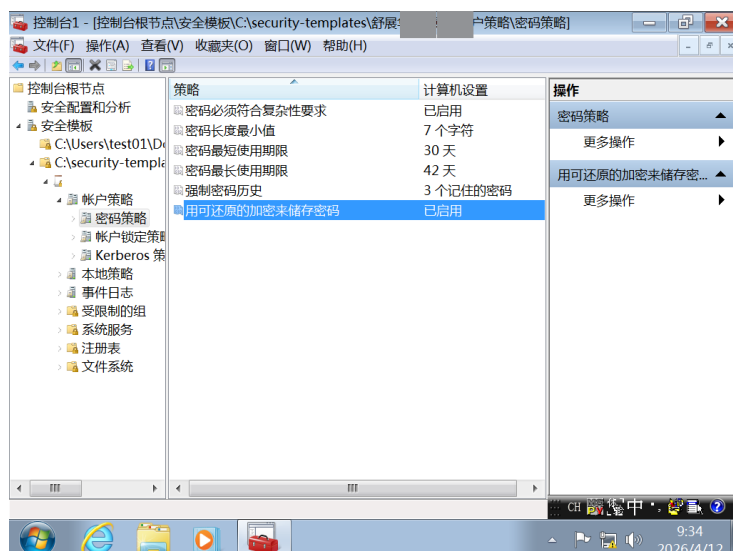


图 24: 完成自定义安全模板的策略设置

(2) 启用安全模板

模板创建完成后，右键查看其“设置描述”，确认模板的基本信息与用途。这一步相当于对模板进行一次复核，便于后续识别当前模板的来源和含义。

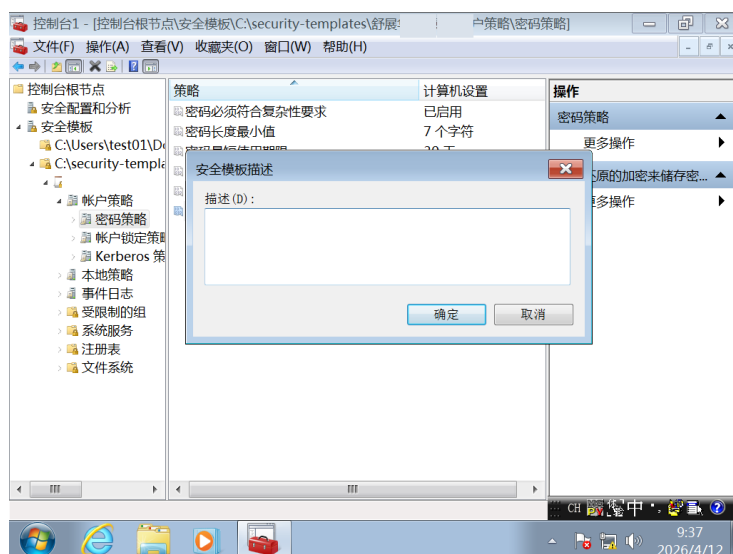


图 25: 查看安全模板的“设置描述”信息

确认无误后，继续在“安全配置和分析”中打开数据库，并把刚才建立的安全模板导入进去。导入数据库后，系统即可基于该模板分析当前计算机的安全状态，并按照模板内容执行配置。

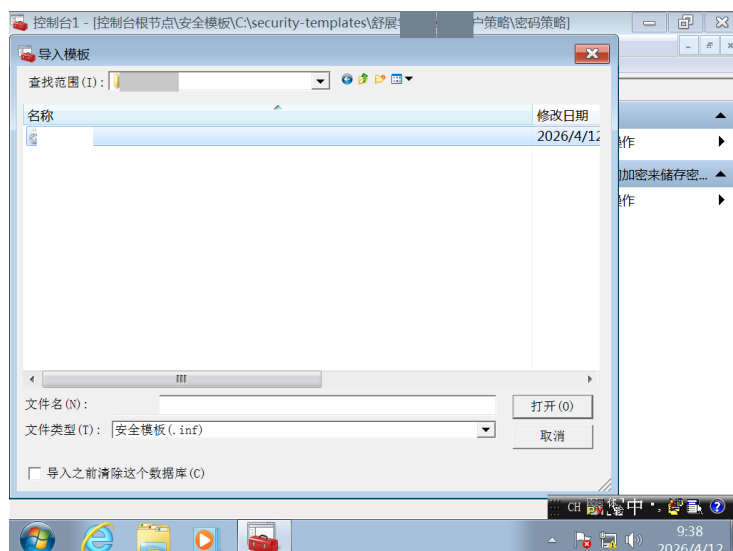


图 26: 新建安全数据库并导入安全模板

模板导入完成后，执行“立即分析计算机”操作，让系统把当前计算机的安全配置和模板内容进行对比分析。通过这一步，可以知道当前系统设置与目标模板之间是否一致，也能看出哪些安全项需要进一步调整。



图 27: 使用“安全配置和分析”分析系统安全设置

最后执行“立即配置计算机”，使系统按照所选模板的要求应用相应配置。虽然该操作过程较快，但从实验界面可以确认这一步已经完成。这样做的实际效果，是把原本需要手工逐项设置的安全参数，转化为可以重复使用的模板配置，提高系统加固的统一性和效率。

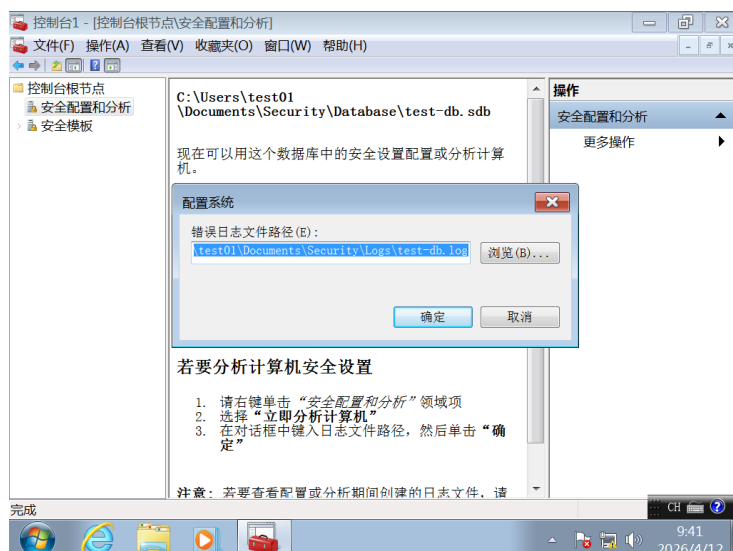


图 28: 执行“立即配置计算机”操作

2. 总结

2.1 对上机实践结果进行分析

从整体过程看，实验依次完成了账户和口令的安全设置、文件加密与证书授权、审核与日志查看、安全模板配置四个环节。完成四部分实验后，各项安全设置之间形成了较清晰的对应关系。账户和口令设置对应登录入口的基础安全；文件加密与证书授权对应数据访问控制；审核与日志功能用于记录关键安全事件；安全模板用于统一分析和实施这些安全设置。

从实验现象来看，Guest 账户被禁用后，默认来宾入口被关闭；加密文件在未授权用户下无法打开，而导入证书后可以成功访问；审核策略启用后，安全日志中能够看到相应记录；安全模板创建并导入数据库后，系统可以对当前安全设置进行分析并按模板实施配置。实验过程覆盖了 Windows 系统中账户、数据、审计和策略模板几个主要安全配置环节。

2.2 上机的心得体会

通过这次上机，对“操作系统安全”的理解不再只停留在概念层面。实验过程显示，账户控制、密码策略、文件加密、日志审计和模板化配置都属于系统安全的基础组成部分。在加密文件实验中，未授权用户无法打开文件，而导入证书后可以访问，文件保护与身份授权之间的关系也因此更加清楚。

2.3 改进意见

如果后续继续完善本实验，可以进一步补充更多模板策略项，例如账户锁定策略、审核对象访问、用户权限分配等内容，使安全模板更接近真实系统的安全基线。另外，若能在实验平台中补充操作前后的登录界面对比或更多安全日志样例，报告中的验证过程会更加完整。