哈尔滨工业大学大学计算机科学与技术学院

《信息安全概论》

实验报告

计算机科学与技术学院

计算机系网络教研室制

|  |  |
| --- | --- |
| 课程名称： | 信息安全概论 |
| 实验名称： | Windows审计策略 |
| 指导教师： | 韩琦 |
| 学生姓名： | 陈三元 |
| 组 号： | 2-28 |
| 实验日期： | 2018.3.25 |
| 实验地点： | 哈尔滨工业大学 |
| 实验成绩： |  |

一、实验目的

1. 学习 Windows 2003 中安全审计策略的配置；
2. 理解 Windows 2003 中审计策略的作用；
3. 掌握 IE 浏览器的安全策略配置；
4. 掌握系统补丁的升级策略配置。

二、实验环境

Windows 2003实验台

三、实验内容与实验要求

1. 打开Windows实验台，运行Windows 2003系统。
2. 进行 Windows 操作系统的帐户策略管理
3. Windows 操作系统中文件操作的审计策略
4. 对 Windows 用户账号管理进行审计
5. 对 Windows 用户登录事件进行审计
6. 对 IE 浏览器进行安全配置
7. 对系统补丁自动升级进行配置

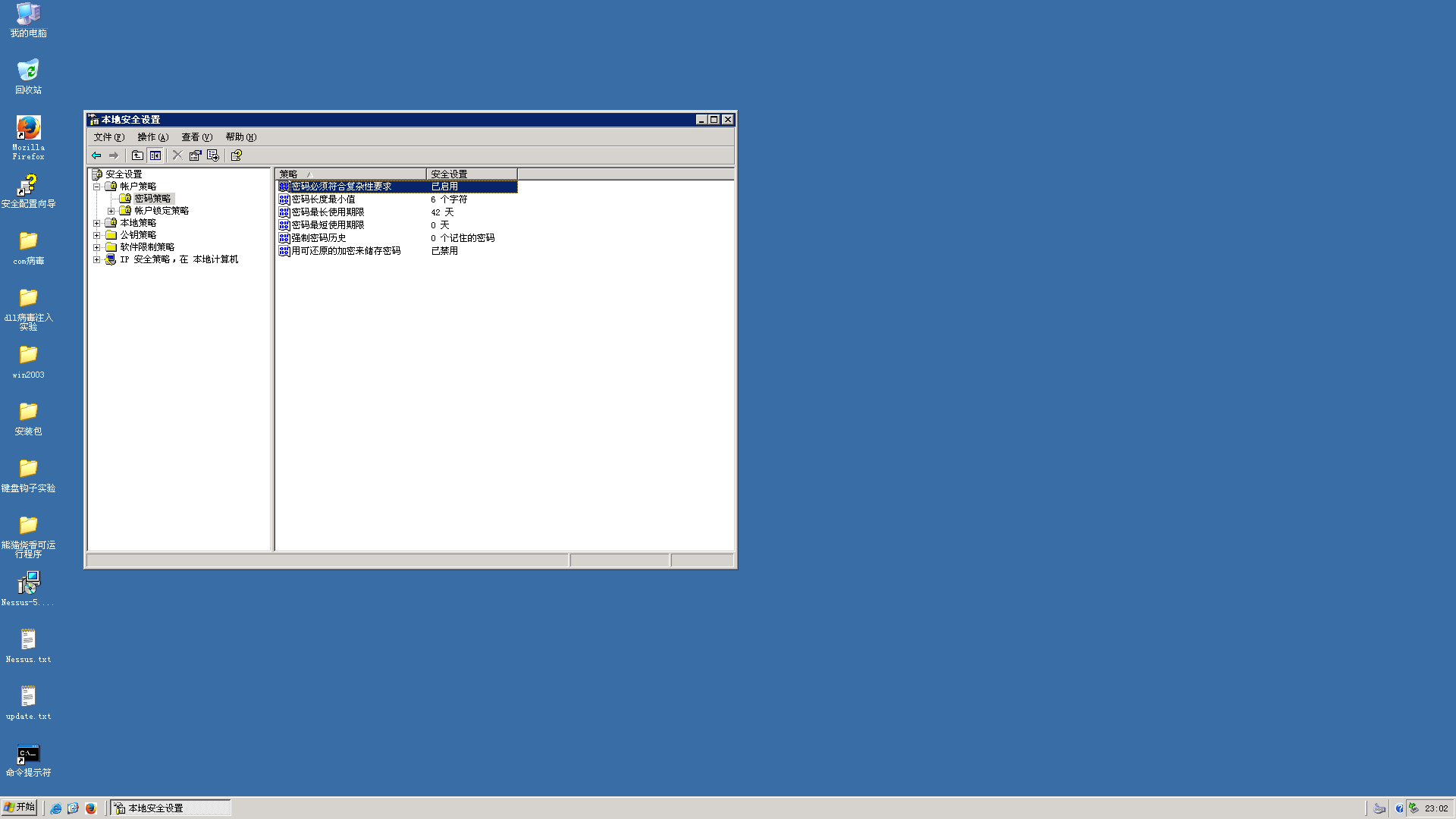
四、实验过程与分析

1. 进行 Windows 操作系统的帐户策略管理

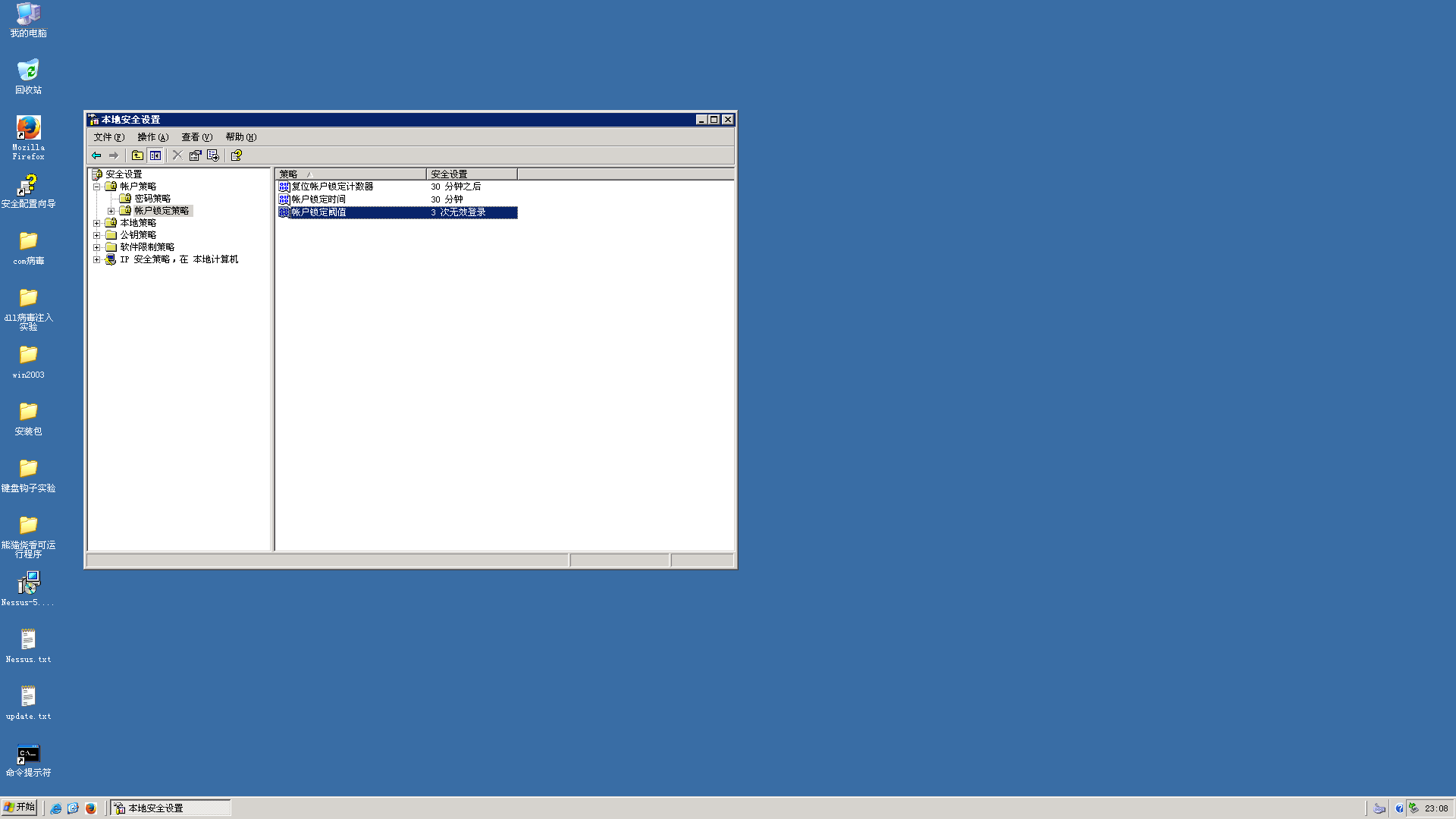
以管理员身份登陆系统，打开“控制面板|管理工具”，运行“本地安全策略”；

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”，设置密码长度的最小值为6；

启用“密码必须符合复杂性要求”功能；

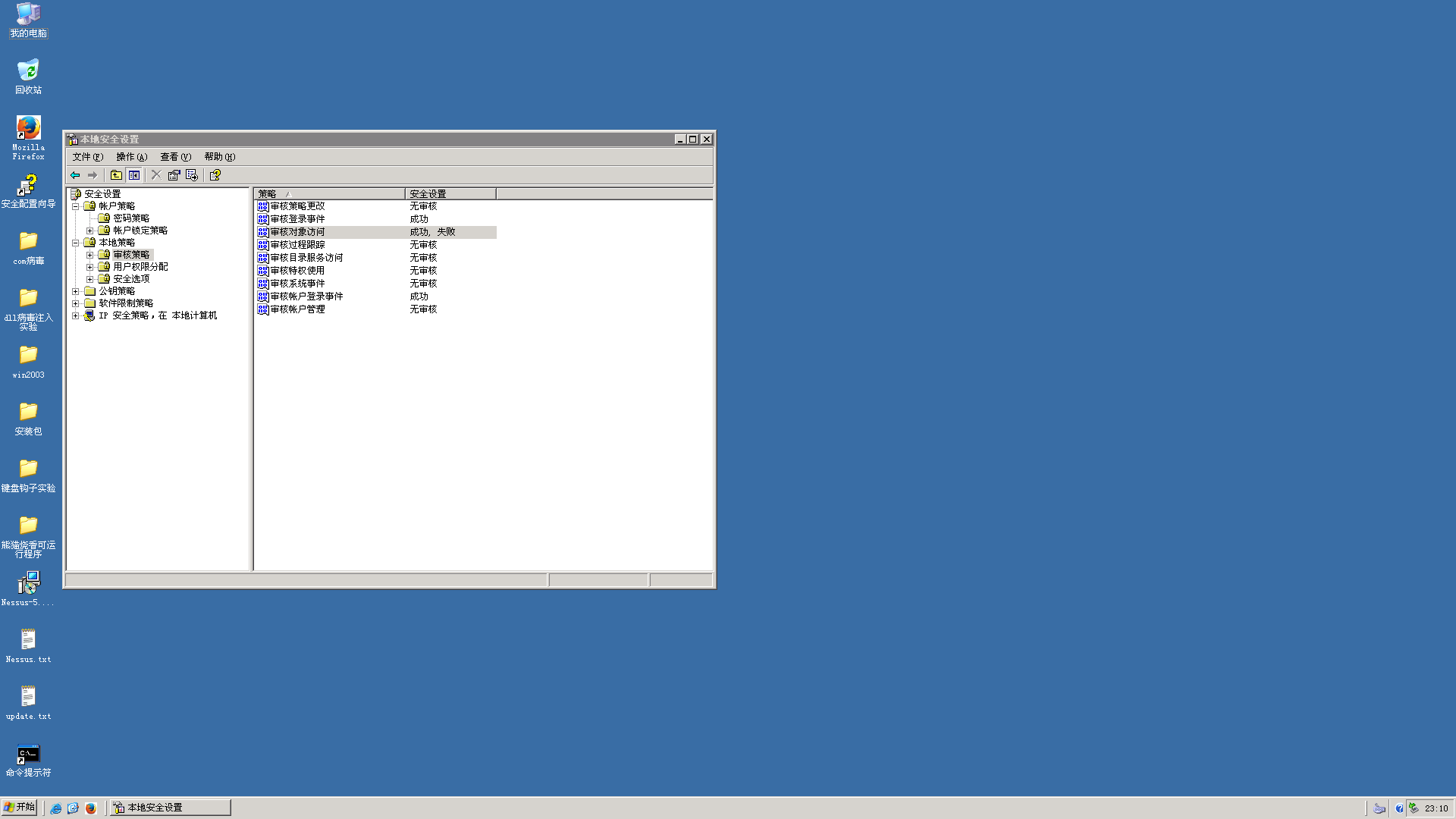


选择“账户锁定策略|账户锁定阈值”，设定最大错误次数为3。

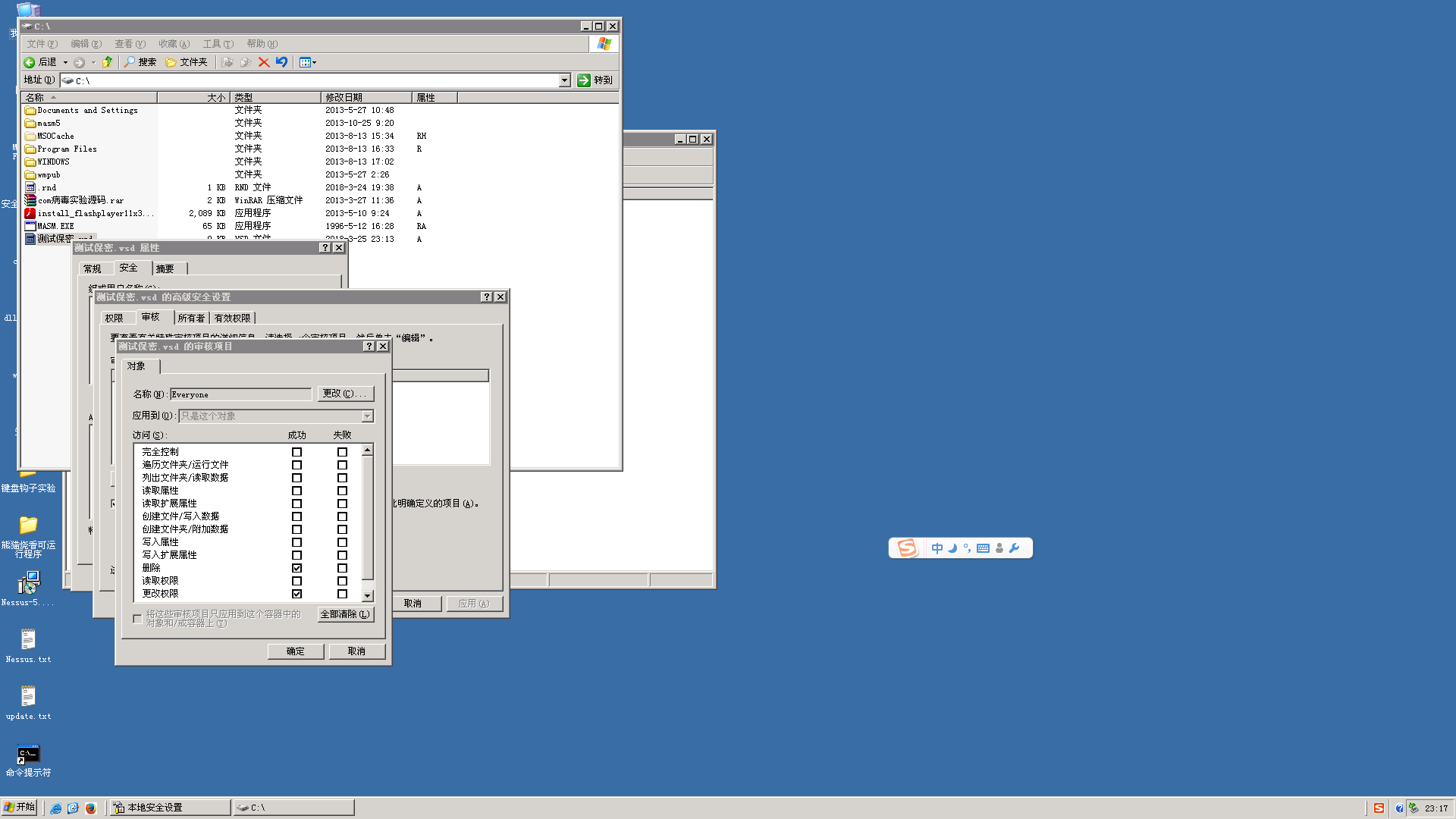


1. Windows 操作系统中文件操作的审计策略

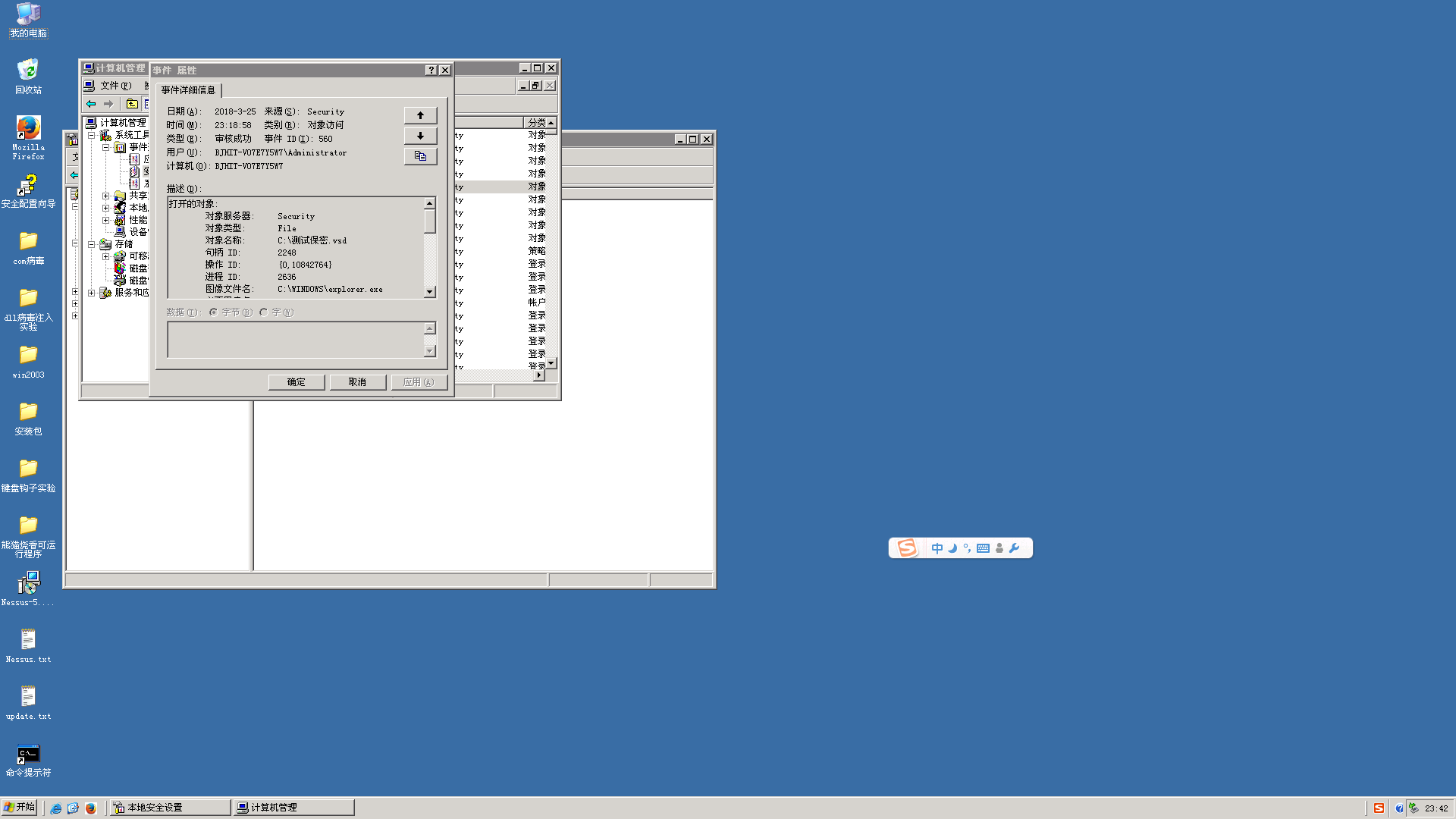
以管理员身份登录系统：打开“控制面板|管理工具”，运行“本地安全策略”；打开“本地安全设置”对话框，选择“本地策略|审核策略”，双击“审核对象访问”，选“成功”和“失败”。



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|高级|审核|添加|高级|立即查找”，找到Everyone，最后选定“删除”和“更改权限”。

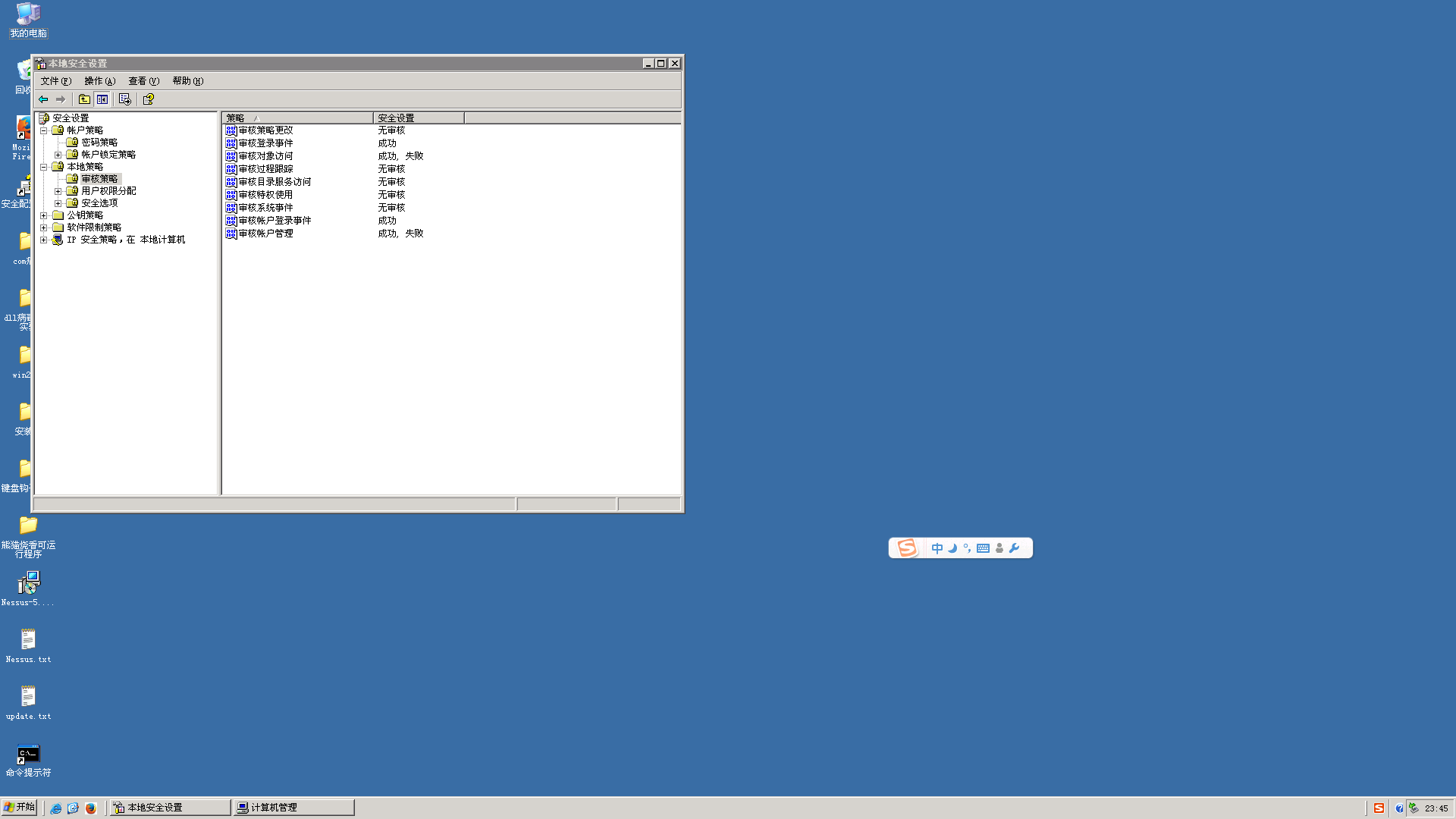


删除“测试保密.vsd”，右键单击桌面上“我的电脑”，选择“管理”，在计算机管理中，选择“系统工具|事件查看器|安全性”，找到删除事件。

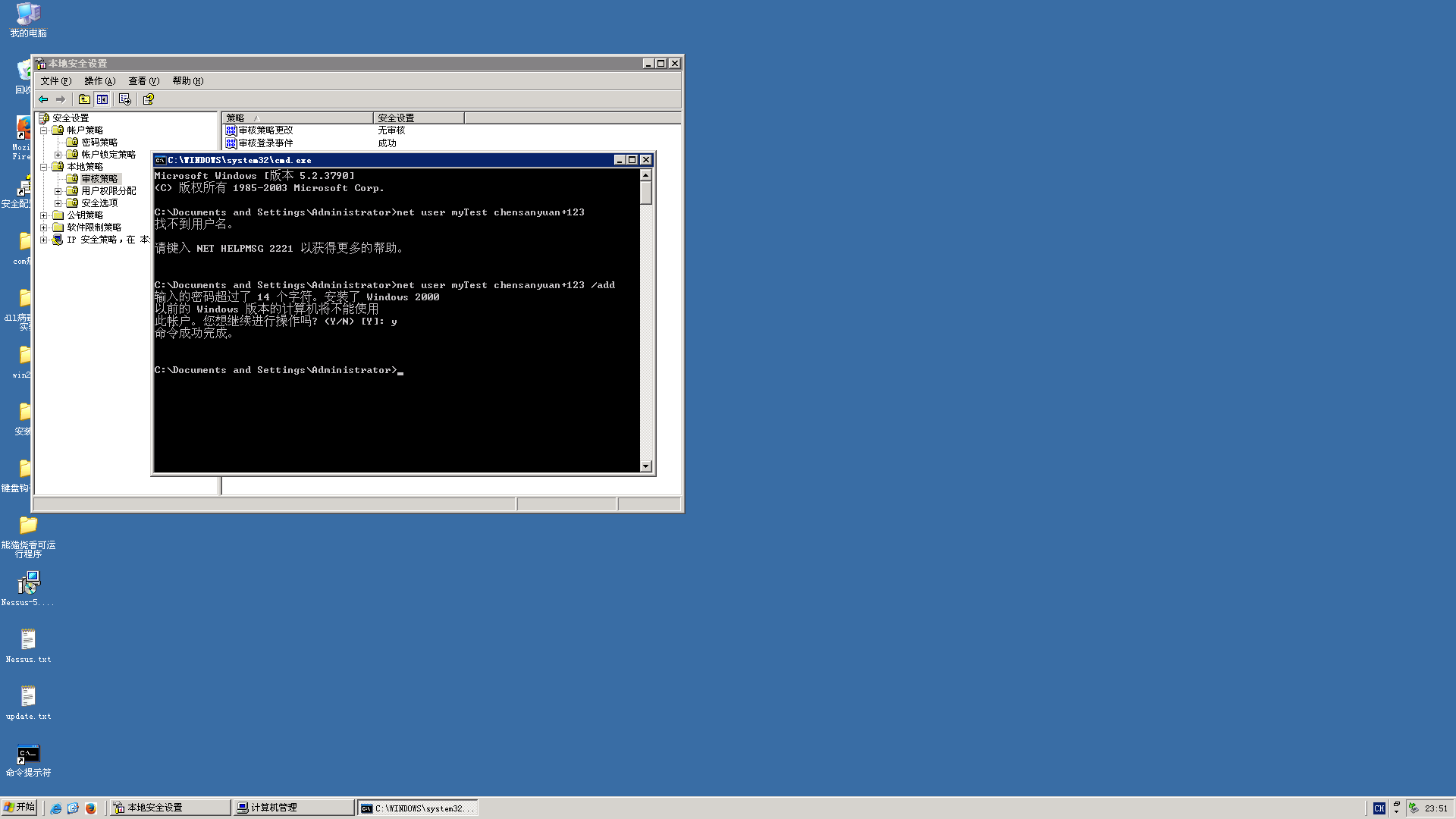


1. 对 Windows 用户账号管理进行审计

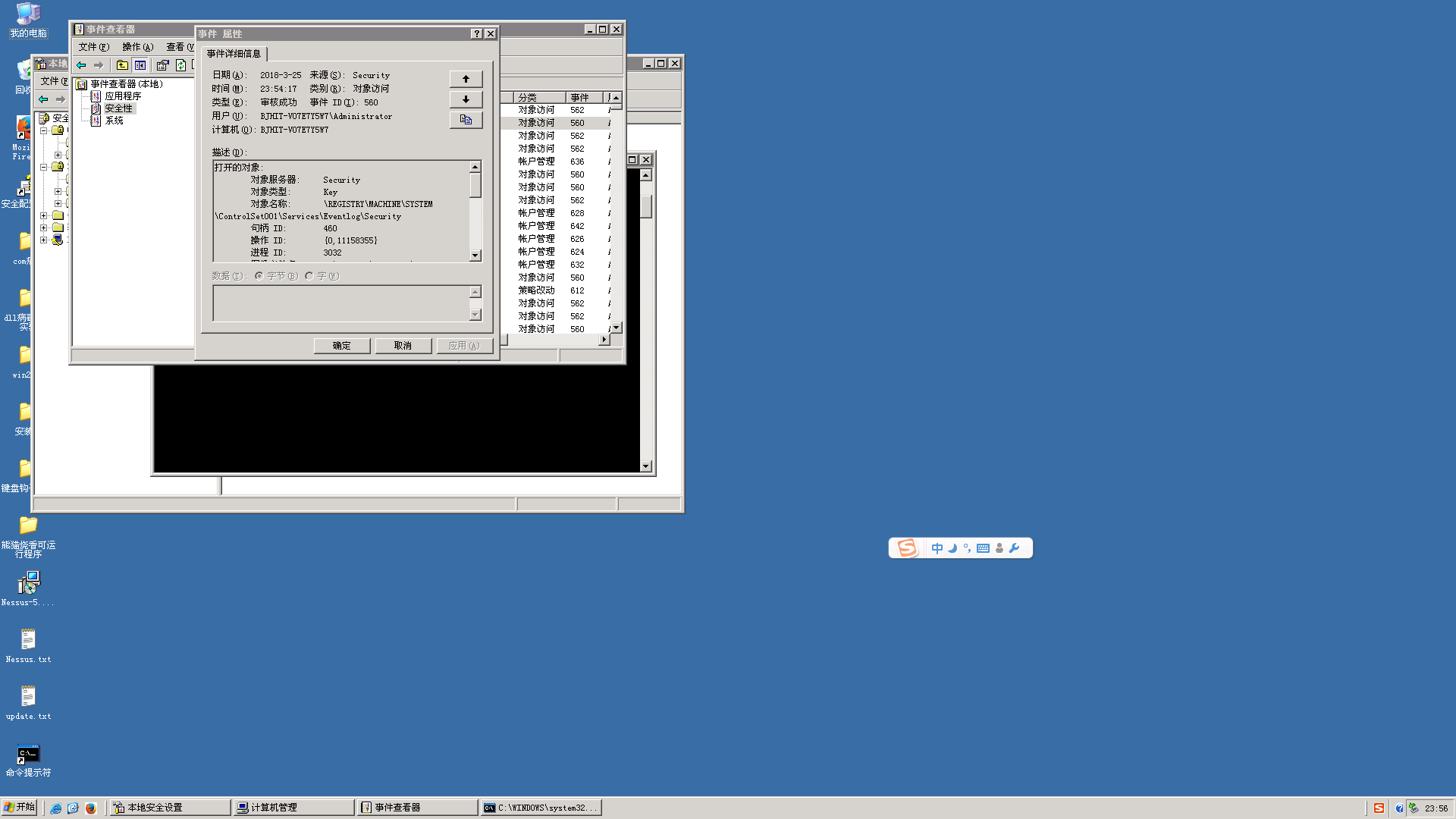
打开“控制面板|管理工具”，运行“本地安全设置”；选择“安全设置|本地策略|审核管理”，双击“审核帐户管理”，选“成功”和“失败”。



在“开始|运行”中，输入 cmd，在控制台下输入net user myTest chensanyuan+123，创建用户 myTest并设置口令为chensanyuan+123。

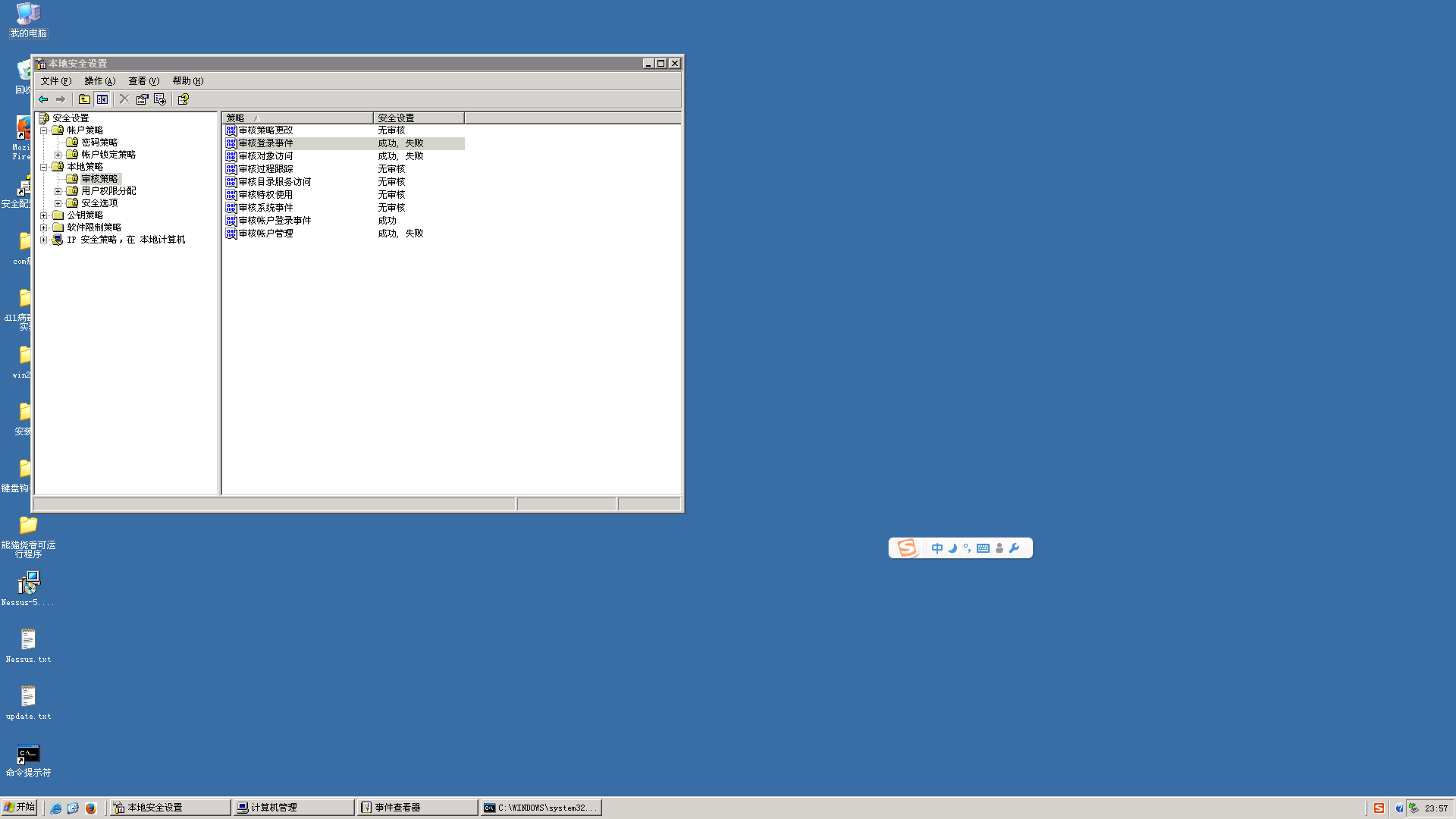


在“开始|运行”中执行 eventvwr.exe，在打开的“事件查看器”窗口中选择“安全性”;



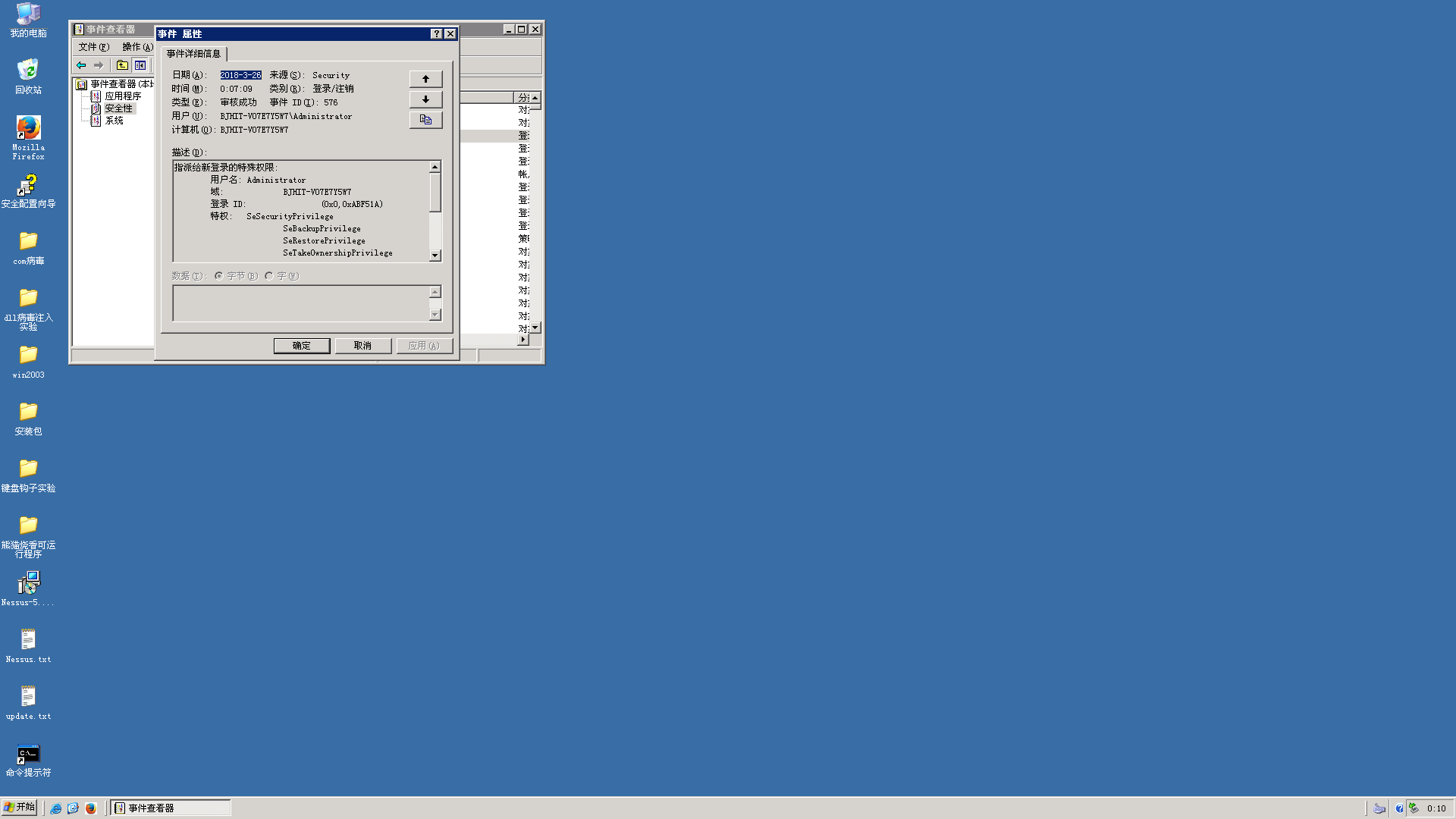
1. 对 Windows 用户登录事件进行审计

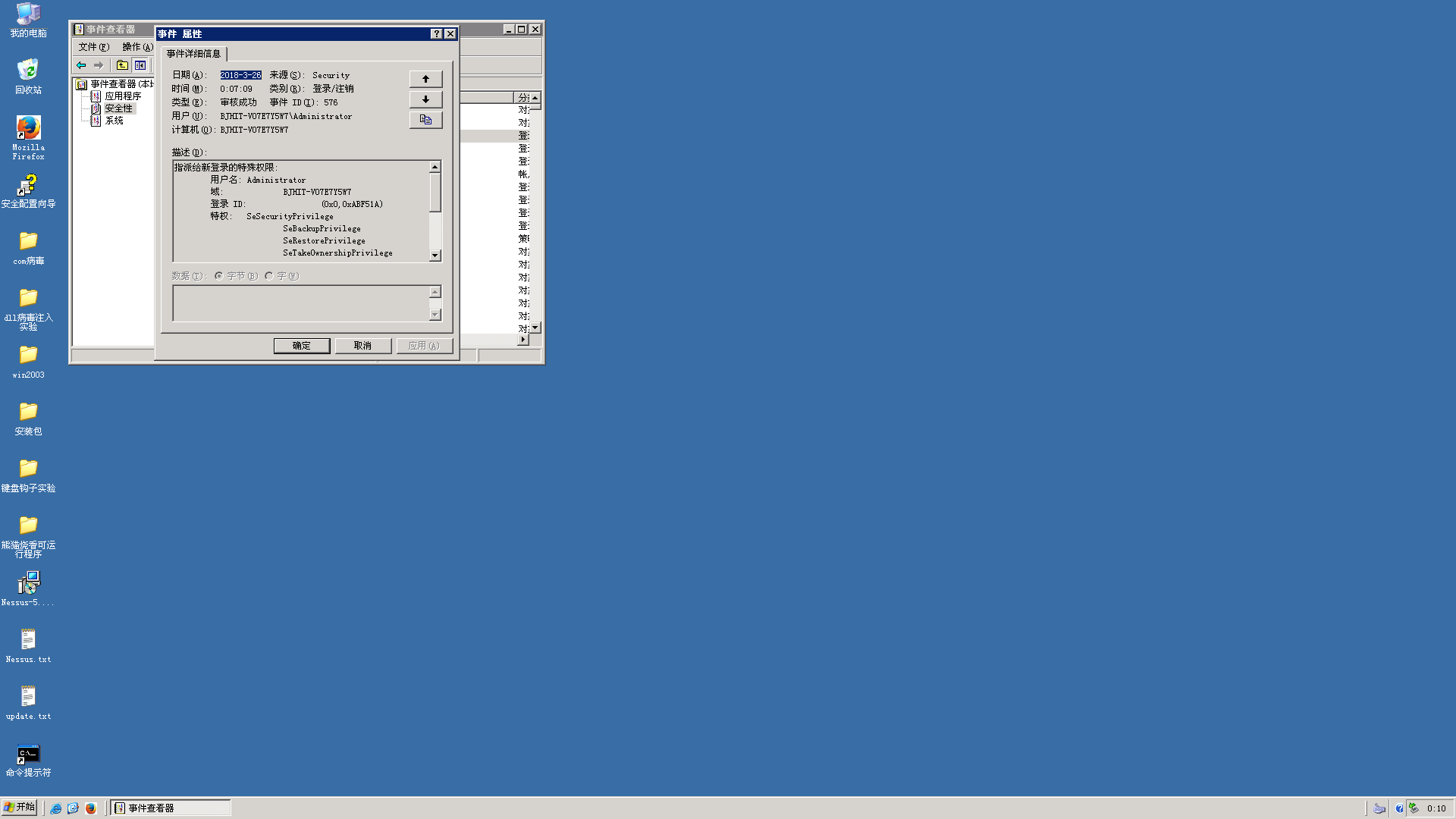
运行“本地安全设置”，选择“安全设置|本地策略|审计策略”，双击“审核帐户登录事件”，选“成功”和“失败”。



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;

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”，可以查看事件记录；

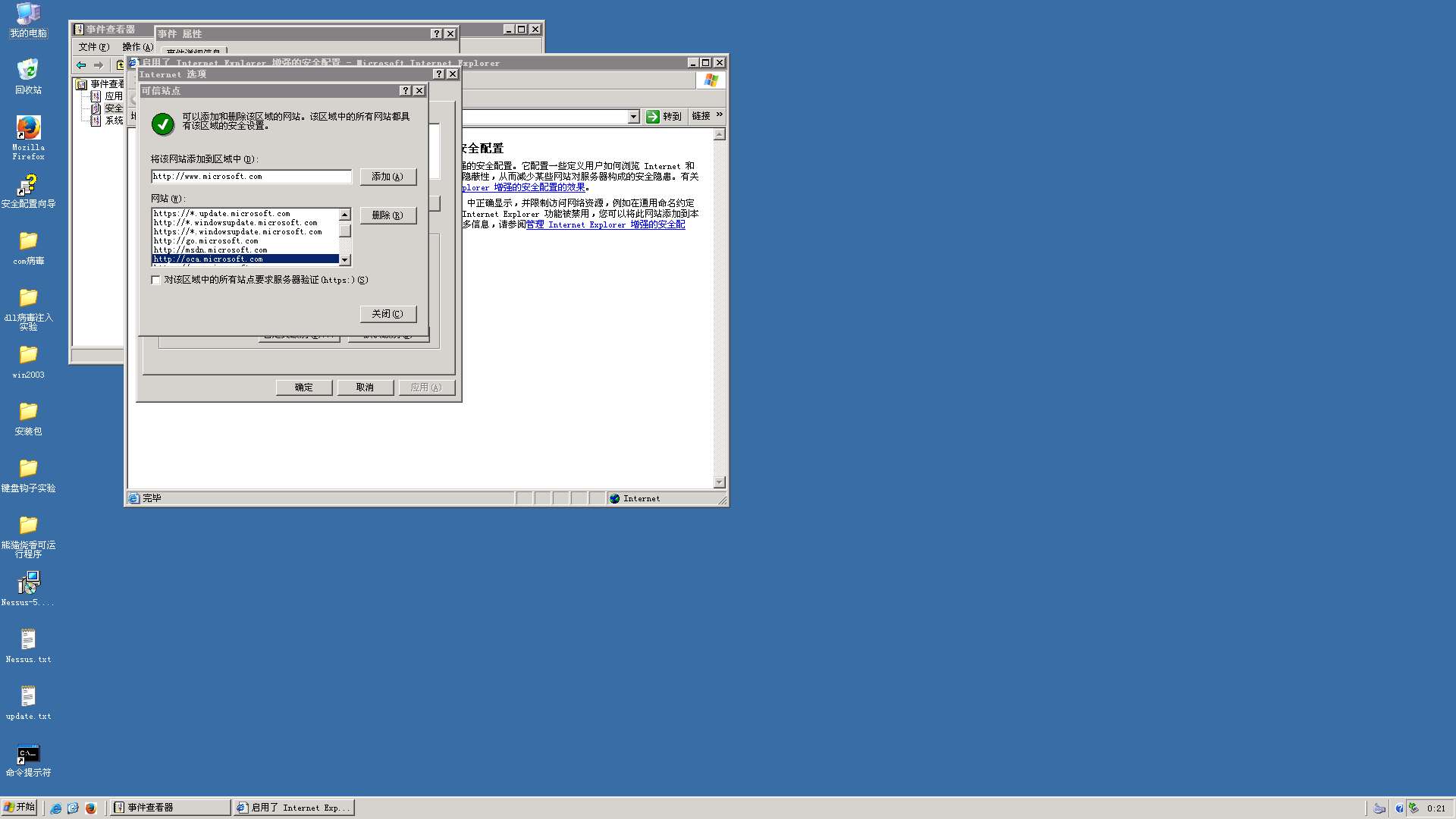




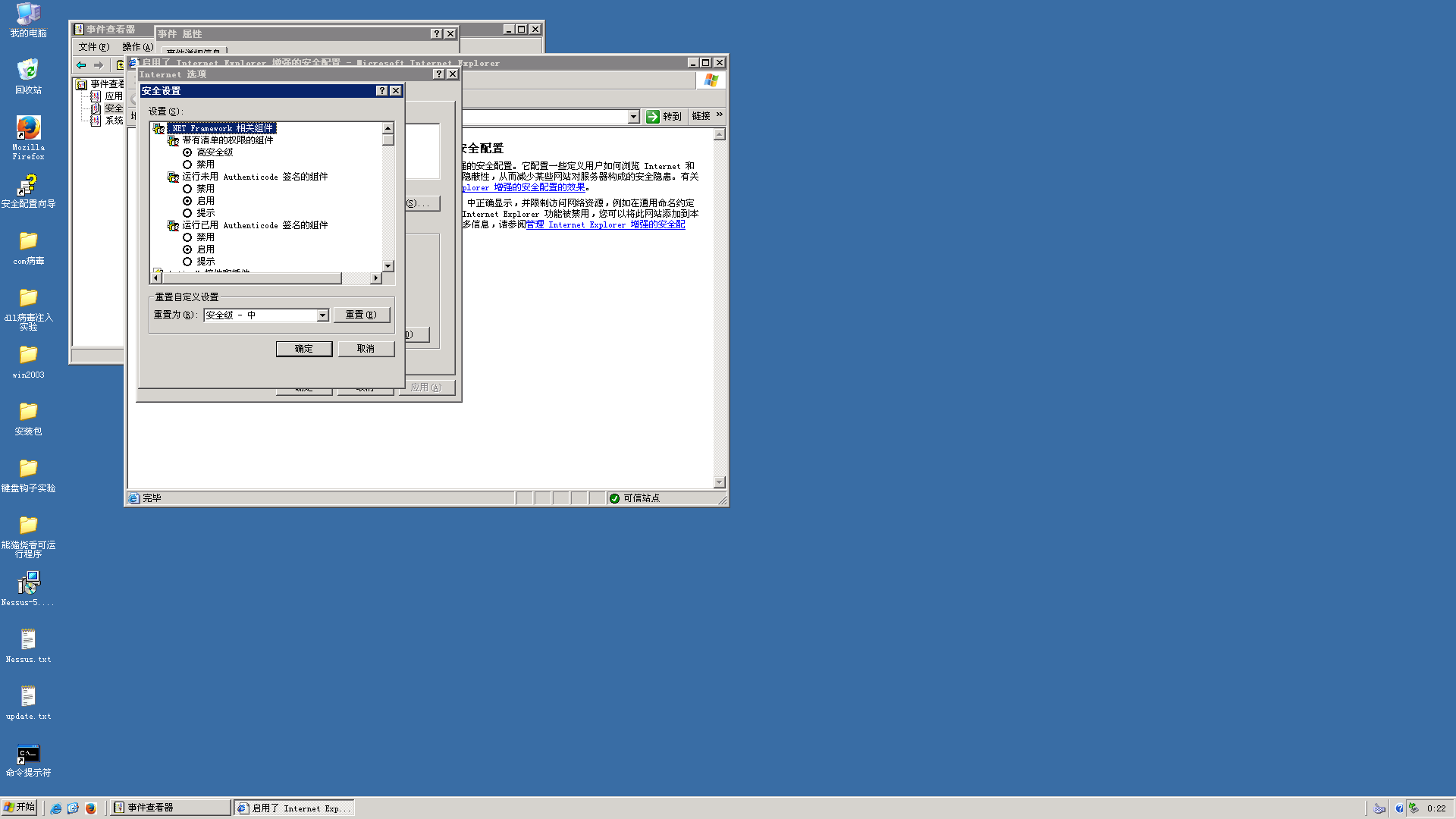
1. 对 IE 浏览器进行安全配置

安全区域设置。

在 IE“工具”菜单上，点击“Internet 选项”，选择“安全”选项卡，在“受信任的站点”中添加可信站点。

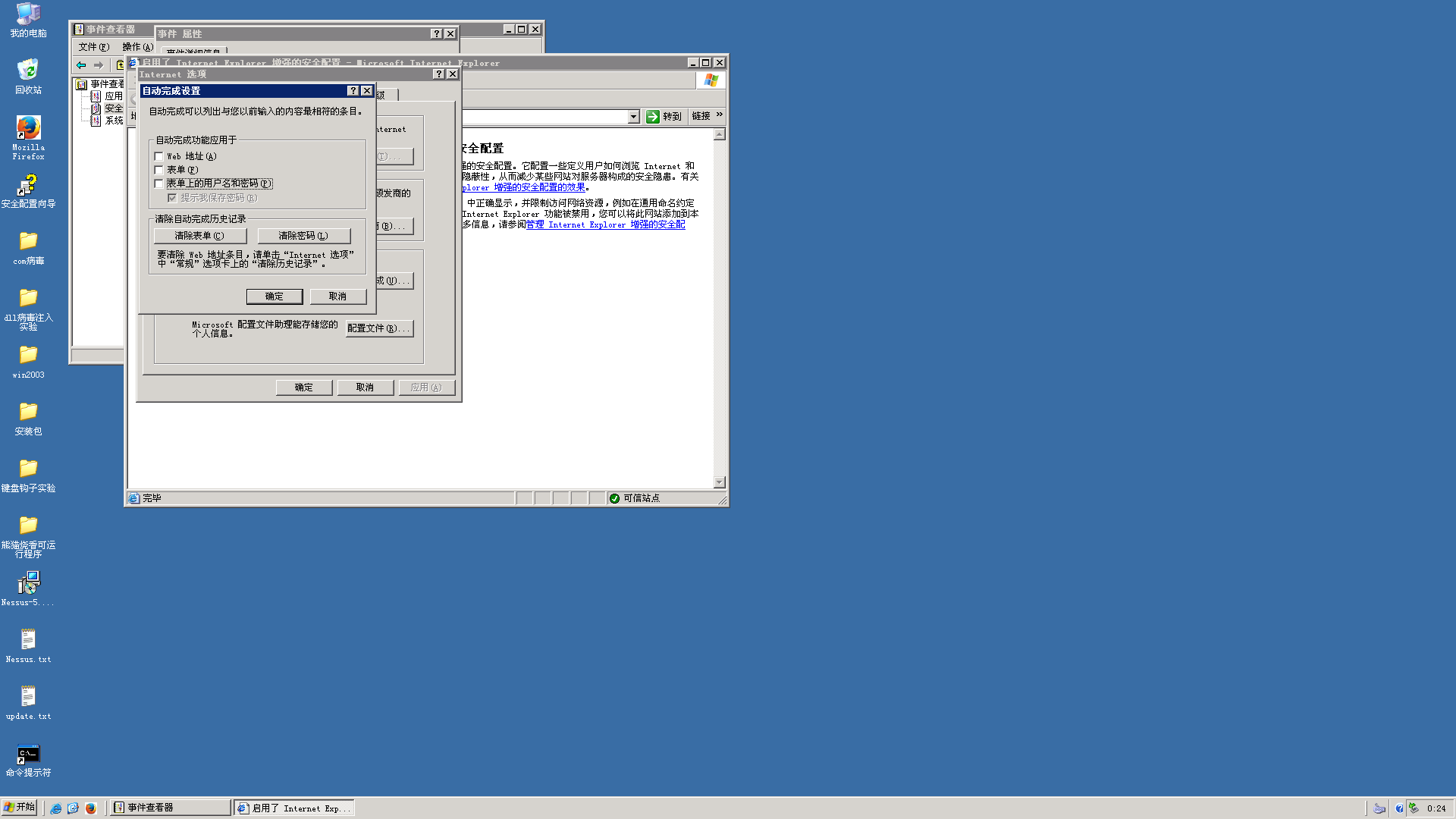


手动更改区域的安全级别。



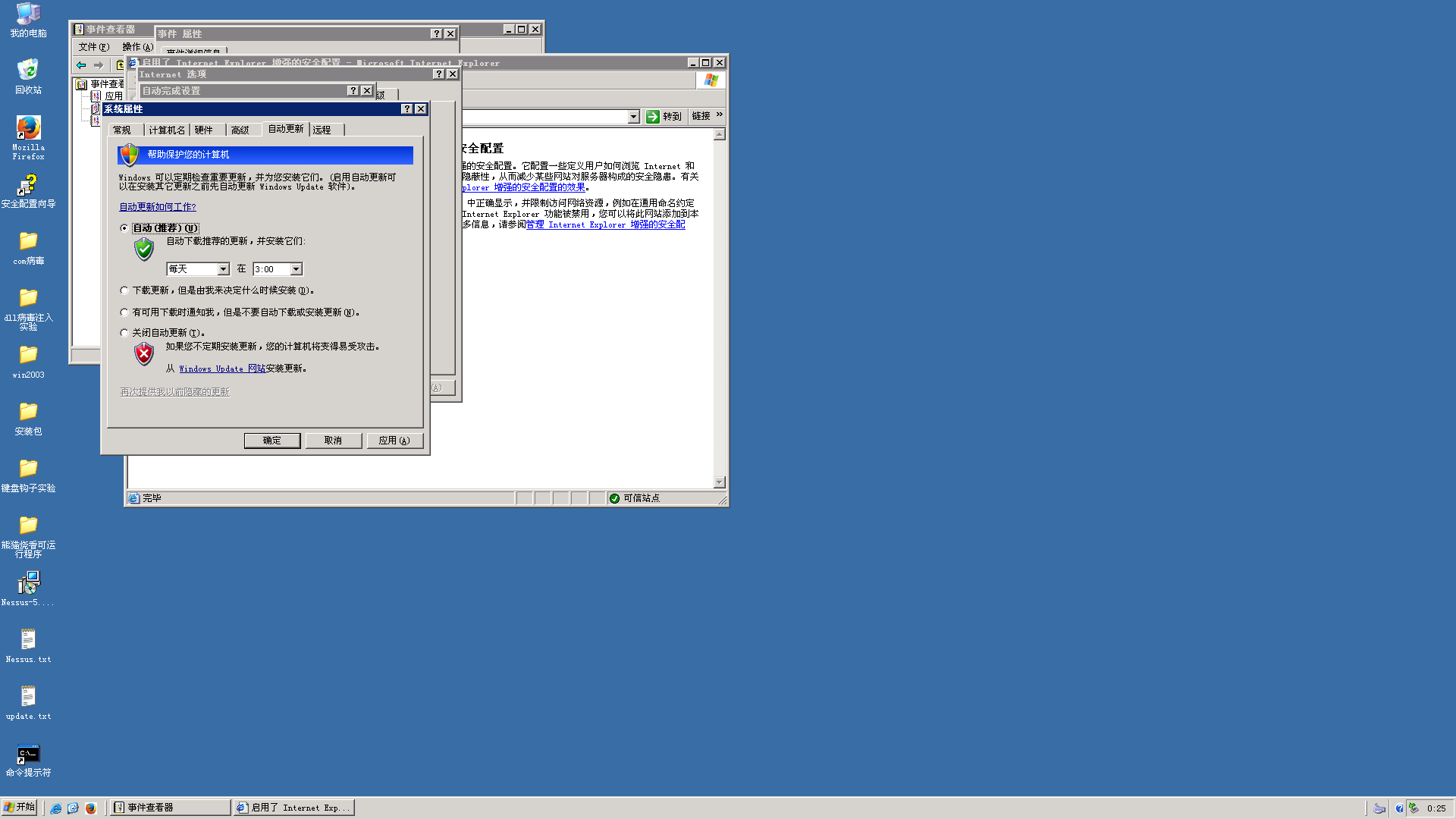
自动完成配置。

在 Internet 选项中选择“内容“标签页，点击“自动完成”按钮，取消所有的自动完成功能。



1. 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，选中“自动”，并选择自动更新时间。



五、实验结果总结

1. 思考 Windows 中审计管理的作用和意义

Windows 中的审计管理通过运用多种技术手段对于Windows系统网络环境中每一个组成部分的系统状态、安全事件、网络活动进行实时的收集和监控，以便集中报警、记录、分析、处理，可以用于保障网络和数据不会因为内部合法用户的不正当操作而造成系统损坏，数据泄露等安全隐患。

1. 详述 Windows 中对账号的审计，及其对登录事件的审计等

（1）Windows对账号的审计：

对所有与管理计算机（配置了审计）的用户数据库中的帐户有关的事件进行审计，具体例子有创建一个用户、将用户添加到一个组、重命名用户账户、为用户账户更改密码。

无论成功或者失败，审核的结果都会对应一个审核项，具体如下表所示：

|  |  |
| --- | --- |
| 帐户管理事件 | 审核项对应描述 |
| 624 | 用户帐户已创建。 |
| 627 | 用户密码已更改。 |
| 628 | 用户密码已设置。 |
| 630 | 用户帐户已删除。 |
| 631 | 全局组已创建。 |
| 632 | 成员已添加到全局组。 |
| 633 | 成员已从全局组中删除。 |
| 634 | 全局组已删除。 |
| 635 | 新的本地组已创建。 |
| 636 | 成员已添加到本地组。 |
| 637 | 成员已从本地组中删除。 |
| 638 | 本地组已删除。 |
| 639 | 本地组帐户已更改。 |
| 641 | 全局组帐户已更改。 |
| 642 | 用户帐户已更改 |
| 643 | 域策略已修改。 |
| 644 | 用户帐户已自动锁定。 |
| 645 | 计算机帐户已创建。 |
| 646 | 计算机帐户已更改。 |
| 647 | 计算机帐户已删除。 |
| 648 | 禁用了安全性的本地安全组已创建。 |
| 649 | 禁用了安全性的本地安全组已更改。 |
| 650 | 成员已添加到禁用了安全性的本地安全组。 |
| 651 | 成员已从禁用了安全性的本地安全组中删除。 |
| 652 | 禁用了安全性的本地组已删除。 |
| 653 | 禁用了安全性的全局组已创建。 |
| 645 | 禁用了安全性的全局组已更改。 |
| 655 | 成员已添加到禁用了安全性的全局组。 |
| 656 | 成员已从禁用了安全性的全局组中删除。 |
| 657 | 禁用了安全性的全局组已删除。 |
| 658 | 启用了安全性的通用组已创建。 |
| 659 | 启用了安全性的通用组已更改。 |
| 660 | 成员已添加到启用了安全性的通用组。 |
| 661 | 成员已从启用了安全性的通用组中删除。 |
| 662 | 启用了安全性的通用组已删除。 |
| 663 | 禁用了安全性的通用组已创建。 |
| 664 | 禁用了安全性的通用组已更改。 |
| 665 | 成员已添加到禁用了安全性的通用组。 |
| 666 | 成员已从禁用了安全性的通用组中删除。 |
| 667 | 禁用了安全性的通用组已删除。 |
| 668 | 组类型已更改。 |
| 684 | 设置管理组的成员的安全描述符。 |
| 685 | 设置管理组的成员的安全描述符。 |

（2）Windows对账户登录的审计

对于登录、注销或者网络连接到电脑的用户的所有事件进行审计。

无论成功或者失败，审核的结果都有对应的审核项，具体如下表所示：

|  |  |
| --- | --- |
| 登录事件 | 描述 |
| 528 | 用户已成功登录到计算机。有关登录类型的信息，请参阅下面的登录类型表。 |
| 529 | 登录失败。尝试登录时，使用的是未知用户名或已知用户名但密码错误。 |
| 530 | 登录失败。尝试登录时，用户帐户在超过允许时间后仍试图进行登录。 |
| 531 | 登录失败。尝试登录时，使用已禁用的帐户。 |
| 532 | 登录失败。尝试登录时，使用已过期的帐户。 |
| 533 | 登录失败。尝试登录时，用户未经允许登录此计算机。 |
| 534 | 登录失败。用户尝试登录的类型未经允许。 |
| 535 | 登录失败。指定帐户的密码已过期。 |
| 536 | 登录失败。网络登录服务未处于活动状态。 |
| 537 | 登录失败。其他原因导致登录尝试失败。 |
| 538 | 用户的注销过程已完成。 |
| 539 | 登录失败。尝试登录时，帐户已锁定。 |
| 540 | 用户已成功登录到网络。 |
| 541 | 主模式 Internet 密钥交换 (IKE) 身份验证已在本地计算机和所列对等身份之间完成（建立安全关联），或者快速模式已建立数据通道。 |
| 542 | 数据通道已终止。 |
| 543 | 主模式已终止。 |
| 544 | 主模式身份验证失败，因为对等未提供有效证书，或者签名未验证。 |
| 545 | 主模式身份验证失败，因 Kerberos 失败或密码无效。 |
| 546 | IKE 安全关联建立失败，因为对等发送的建议无效。接收的数据包包含的数据无效。 |
| 547 | IKE 握手期间发生故障。 |
| 548 | 登录失败。受信任域的安全 ID (SID) 不匹配客户端的帐户域 SID。 |
| 549 | 登录失败。跨林进行身份验证期间，对应于不受信任的命名空间的所有 SID 都已筛选出来。 |
| 550 | 表明可能存在拒绝服务攻击的通知消息。 |
| 551 | 用户已启动注销过程。 |
| 552 | 在已经以其他用户身份登录的情况下，用户使用显式凭据成功登录到计算机。 |
| 682 | 用户已重新连接到断开连接的终端服务器会话。 |
| 683 | 用户在未注销的情况下断开了终端服务器会话的连接。 |