哈尔滨工业大学

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： | 马玉坤 |
| 组 号： | 3-19 |
| 实验日期： | 2018年3月27日-2018年3月28日 |
| 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 实验台。

网络拓扑见下图：



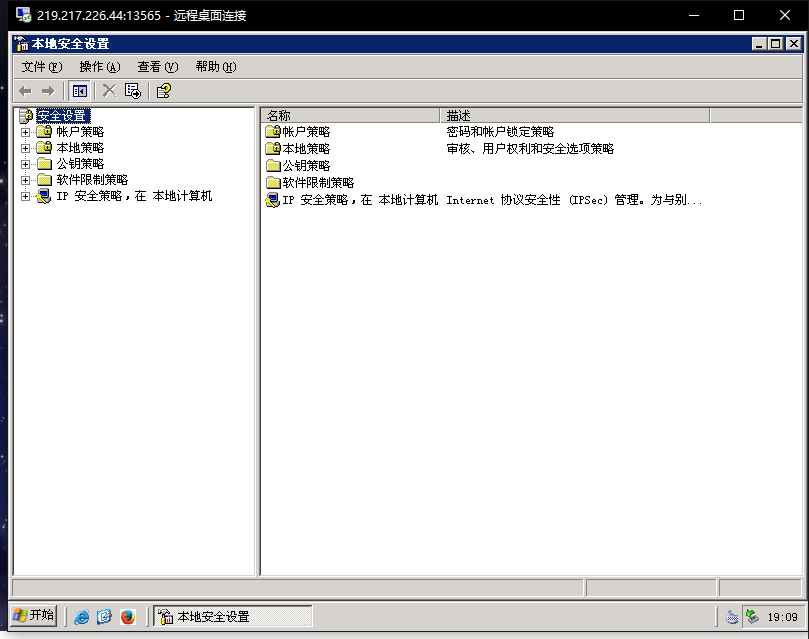
三、实验内容与实验要求

1. 准备工作：打开 Windows 实验台，运行 Windows 2003 系统。
2. 任务一：进行 Windows 操作系统的帐户策略管理
3. 任务二：Windows 操作系统中文件操作的审计策略
4. 任务三：对 Windows 用户账号管理进行审计
5. 任务四：对 Windows 用户登录事件进行审计
6. 任务五：对 IE 浏览器进行安全配置
7. 任务六：对系统补丁自动升级进行配置

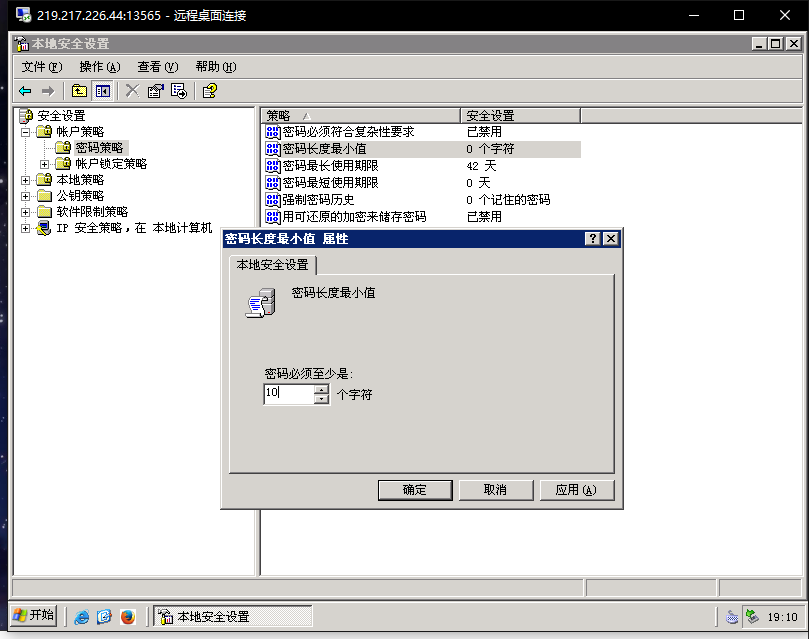
四、实验过程与分析

**任务1：进行 Windows 操作系统的帐户策略管理**

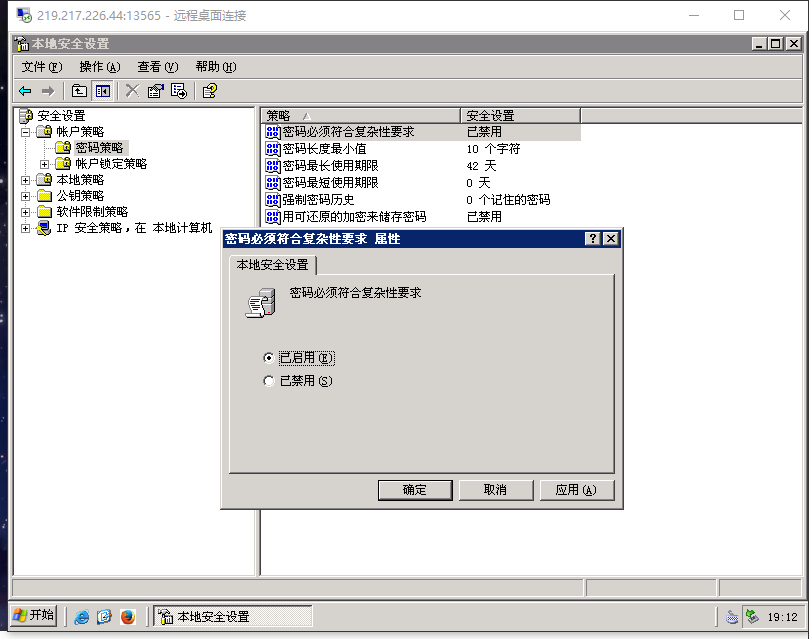
1. **以管理员登录系统，打开“本地安全策略”**



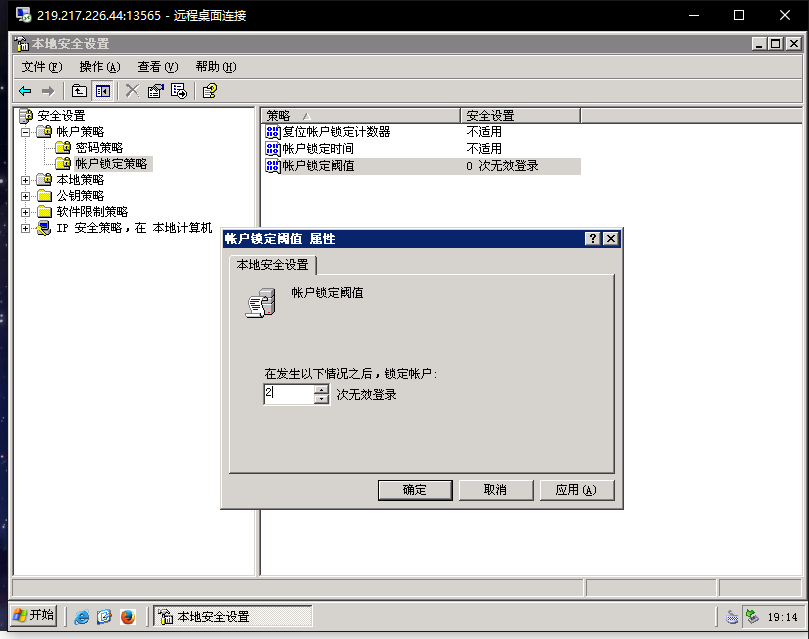
1. **选择账户策略-密码策略-密码长度最小值，设置密码长度最小值**



1. **打开“密码必须符合复杂性要求 属性”窗口，启用该功能**

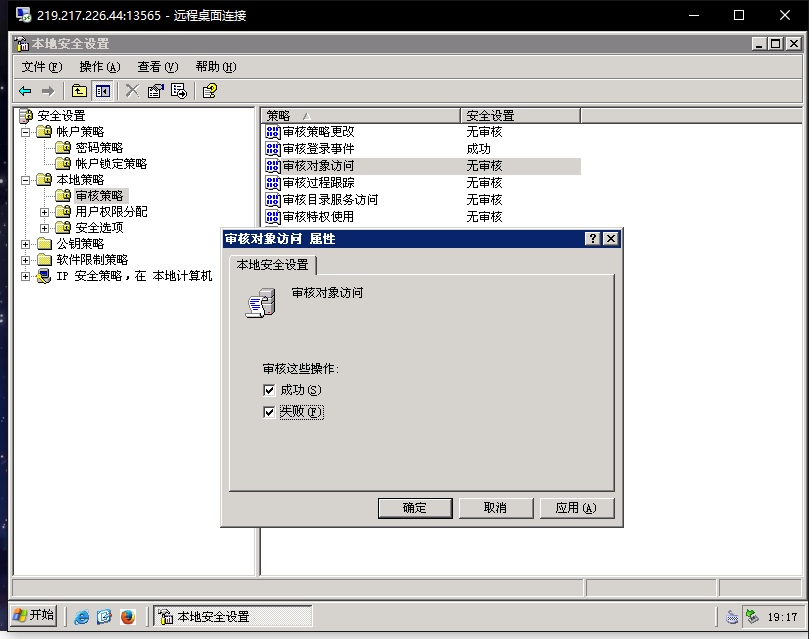


1. **打开“账户策略”-“账户锁定策略”-“账户锁定阈值”，修改数字，设置若干次无效登录后锁定账户**

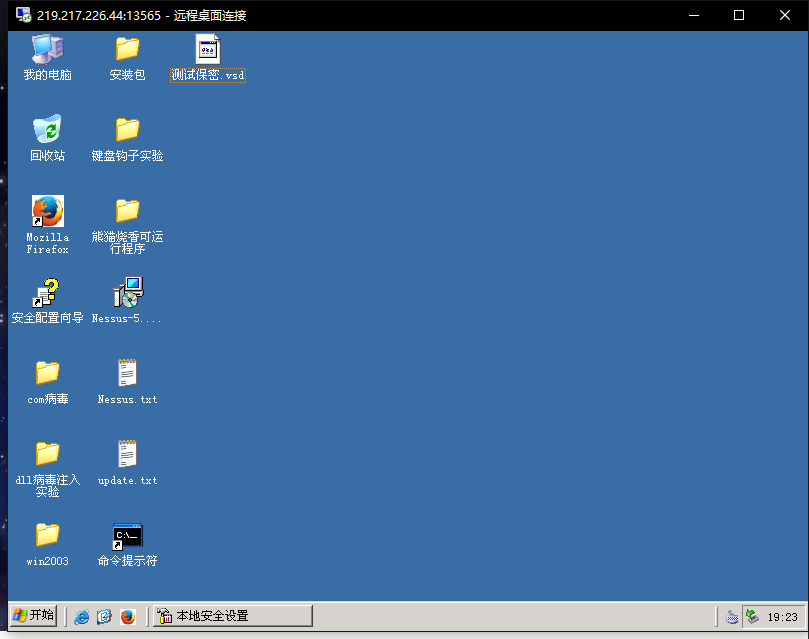


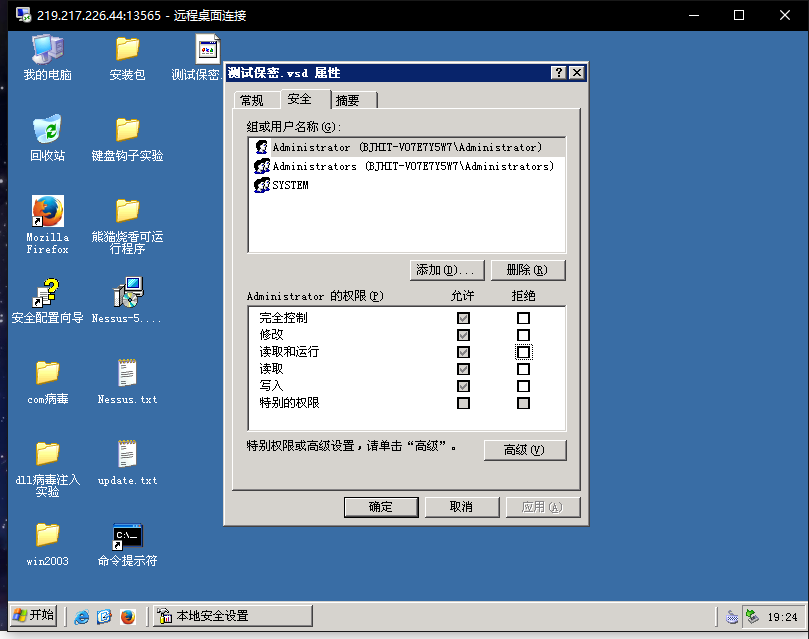
**任务二：Windows 操作系统中文件操作的审计策略**

1. 打开“本地安全策略”，选择“本地策略”-“审核策略”，双击“审核对象访问”，选择“成功”与“失败”。

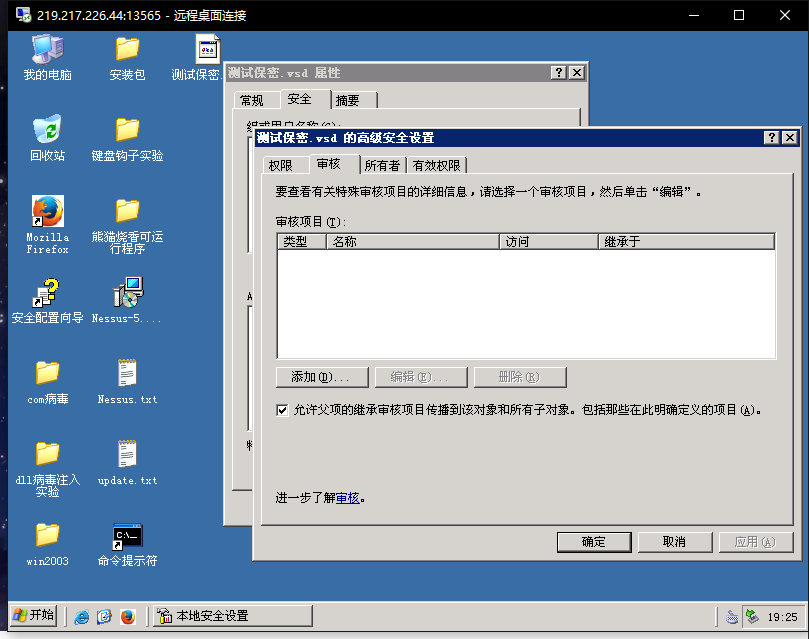


1. 在硬盘上新建“测试保密.vsd”，在文件上按右键，选择“属性”，打开“安全”选项卡

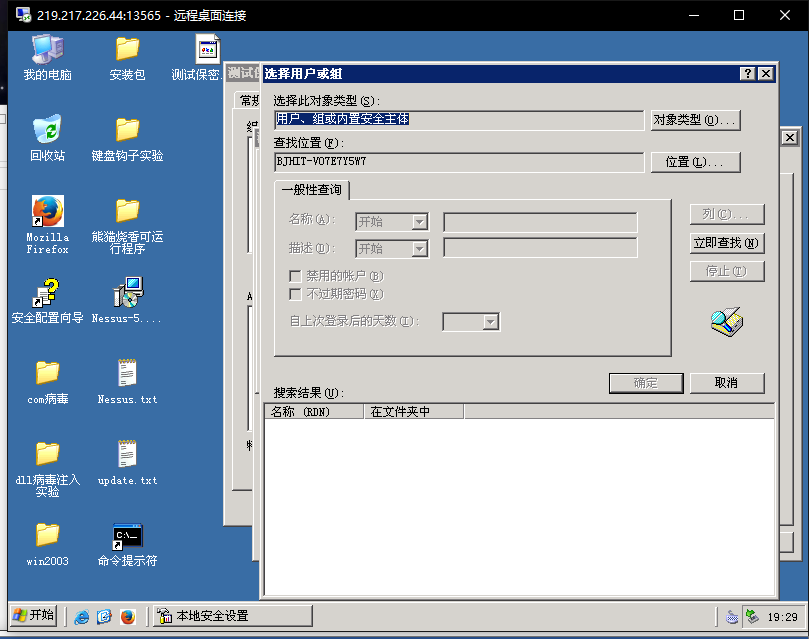


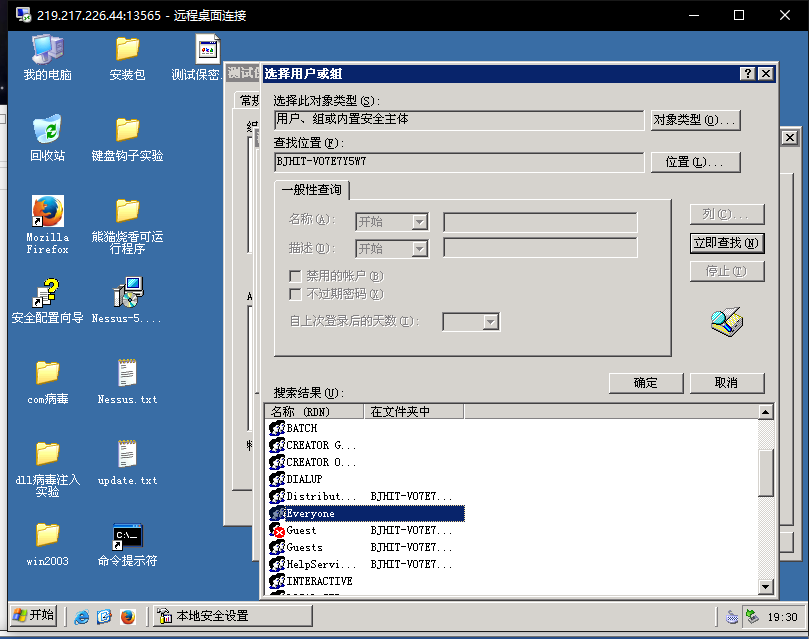


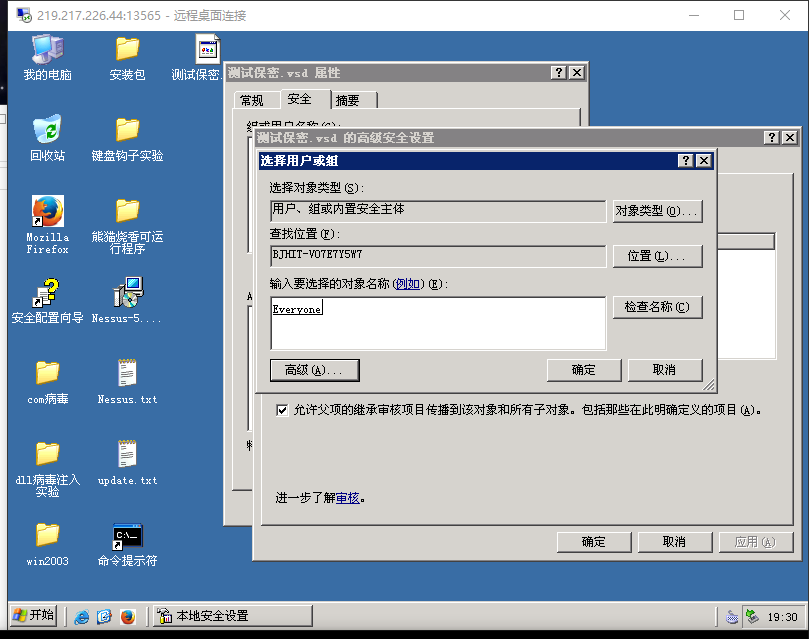
1. 点击“高级”，选择“审核”选项卡



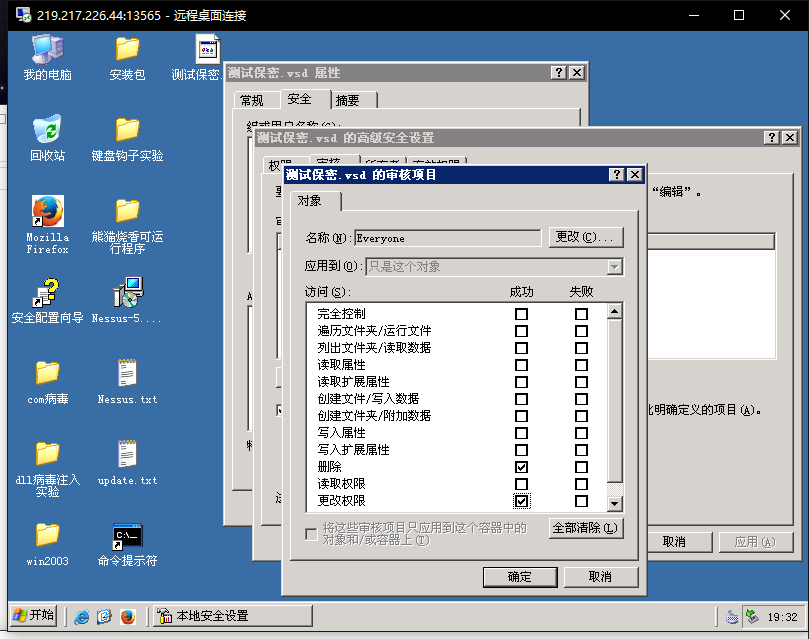
1. 单击“添加”按钮，然后单击“高级”按钮。在“选择用户或组”中点击“立即查找”，搜索结果中选择“Everyone”，然后点击“确定”。

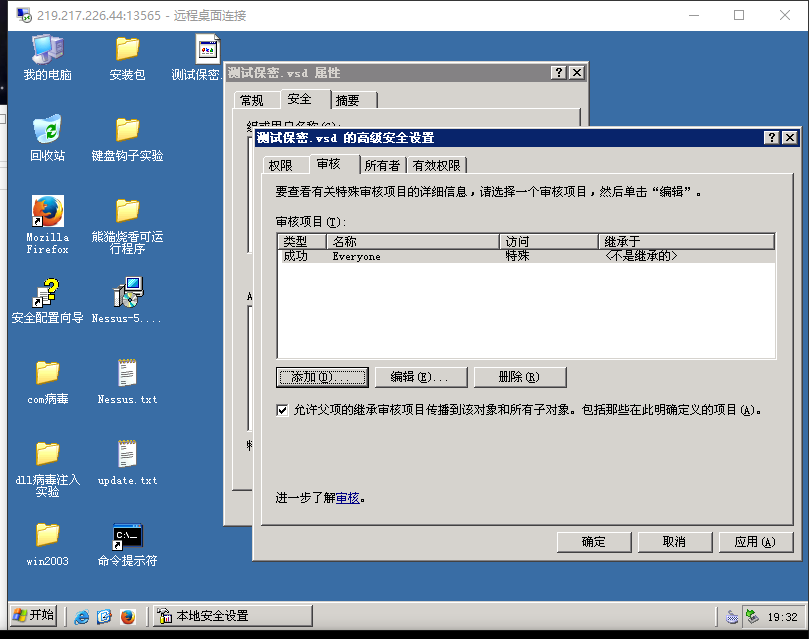


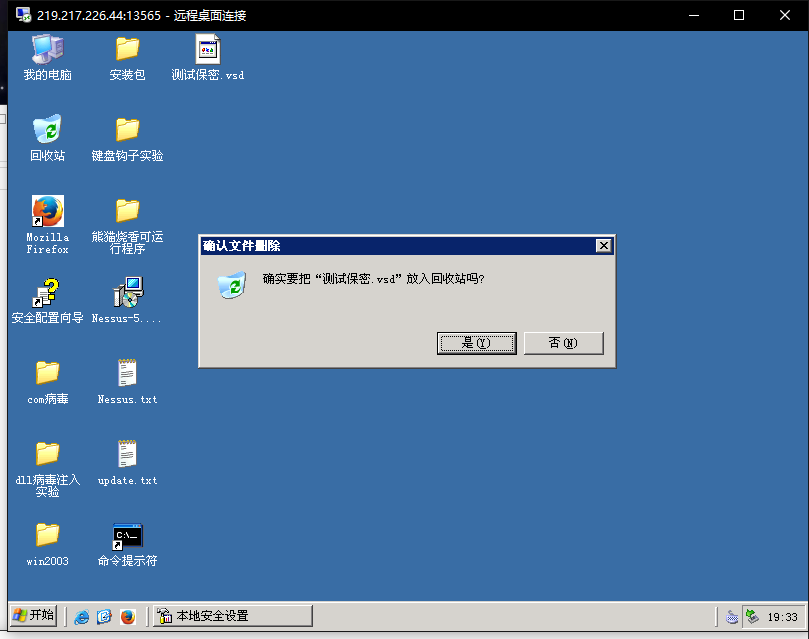




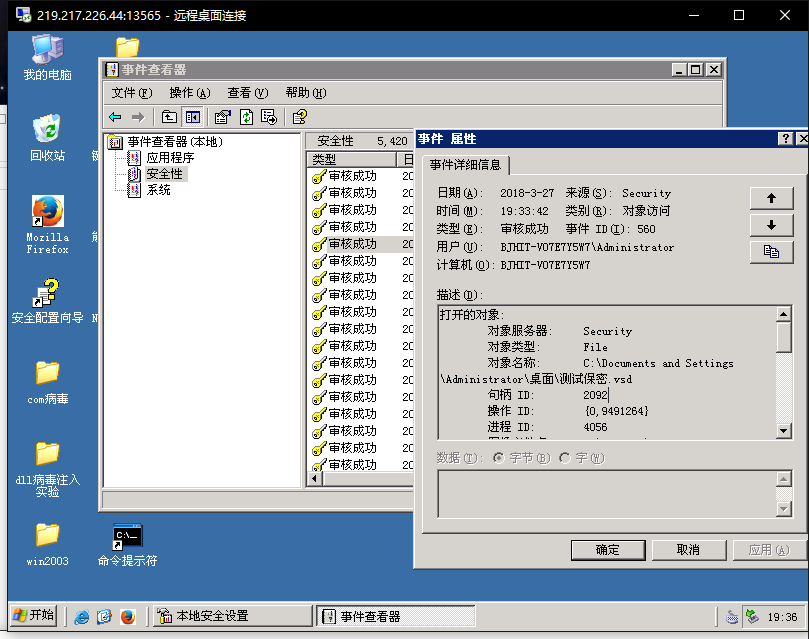
1. 在“测试保密.vsd 的审核项目”对话框中，选择访问中的“删除”和“更改权限”的功能；设置成功后删除该文件。





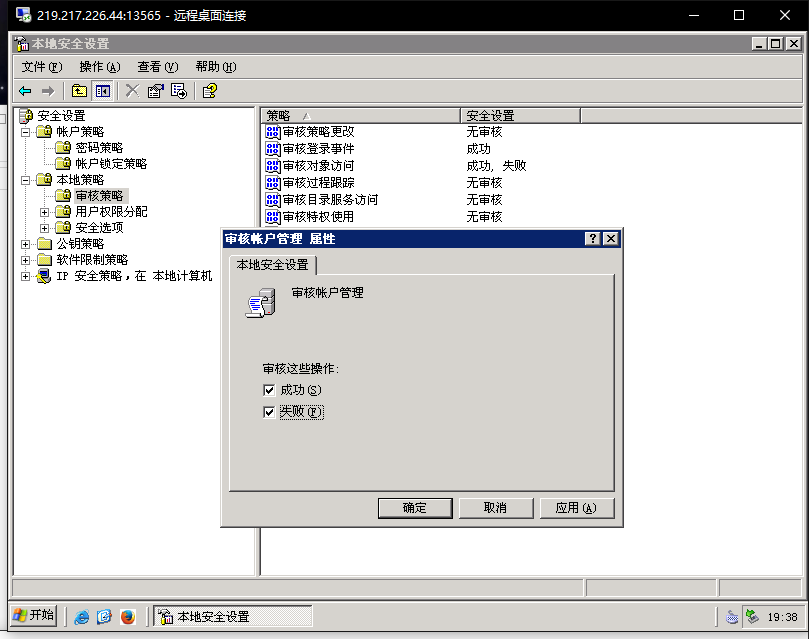


1. 在“开始”-“运行”中输入“eventvwr.exe”，点击“确定”。点击左侧的“安全性”，可以看到删除该文件的事件

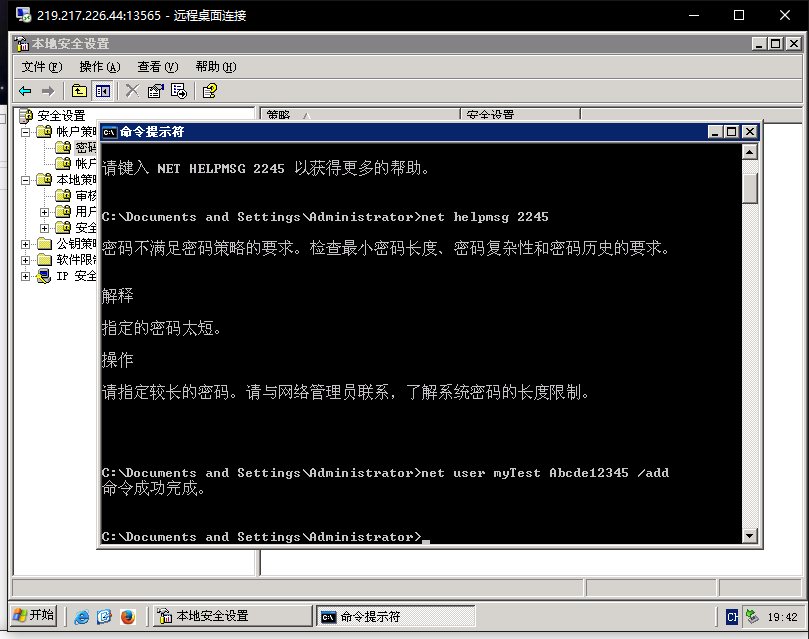


任务三：对 Windows 用户账号管理进行审计

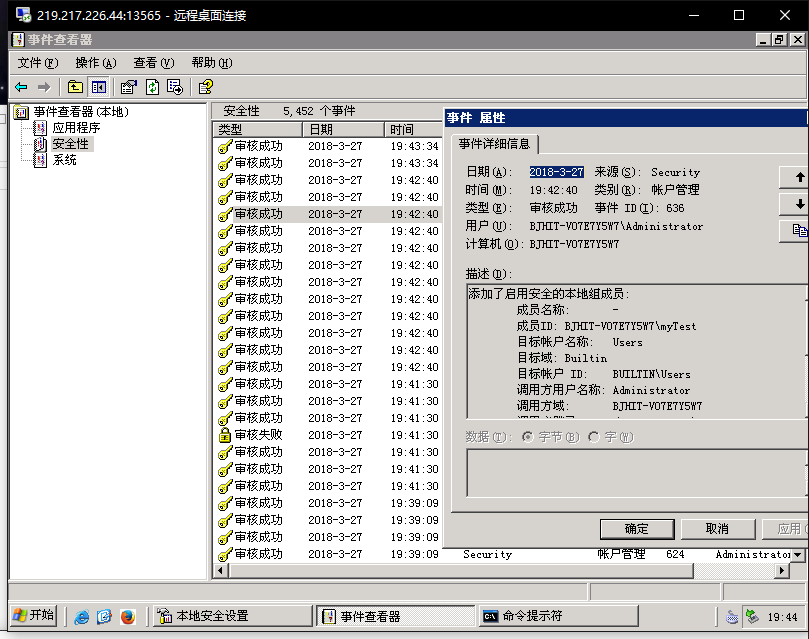
1. 打开“本地安全设置”，选择“安全设置”-“本地策略”-“审核策略”，双击“审核账户管理”，选择“成功”和“失败”。



1. 打开命令提示符，输入创建用户myTest和设置口令的命令。

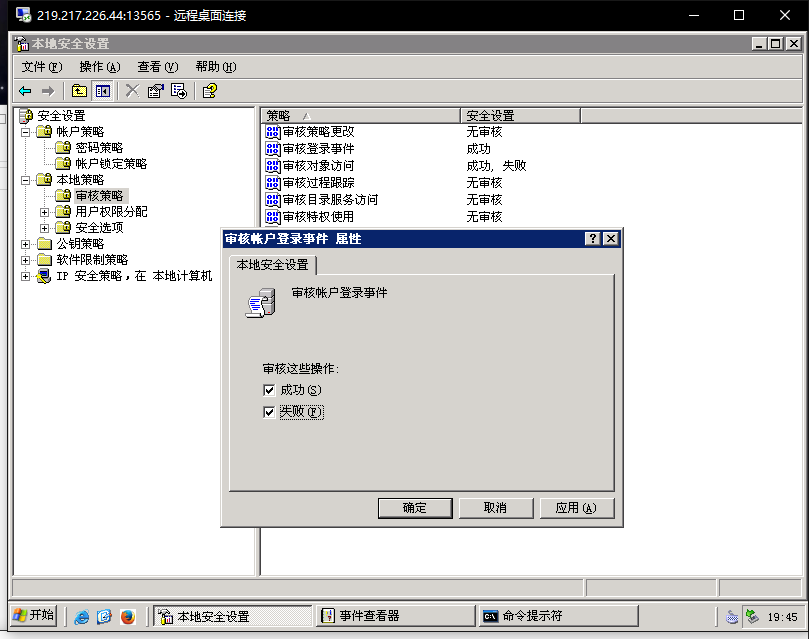


1. 在“运行”窗口中输入eventvwr.exe，然后点击“确定”。在打开的“事件查看器”窗口中选择“安全性”，可以看到该事件

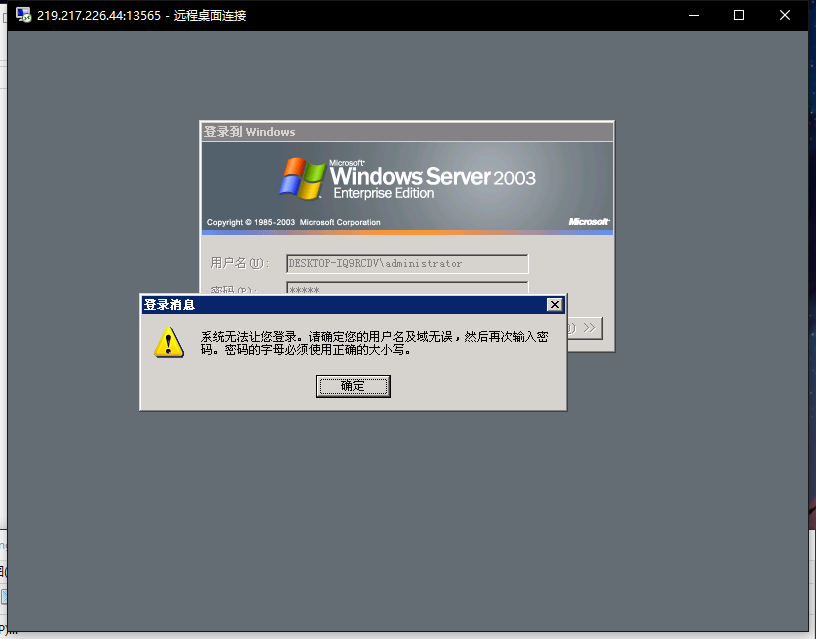


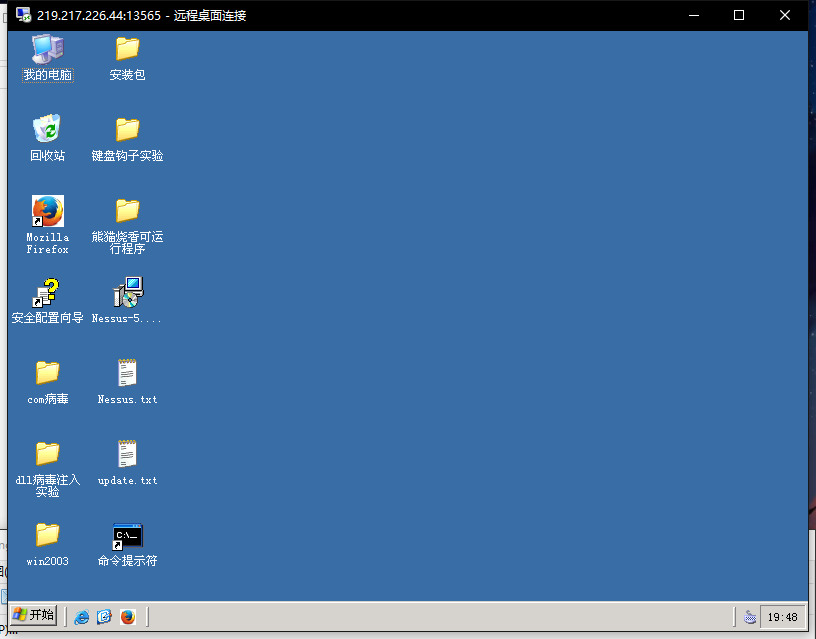
任务四：对 Windows 用户登录事件进行审计

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

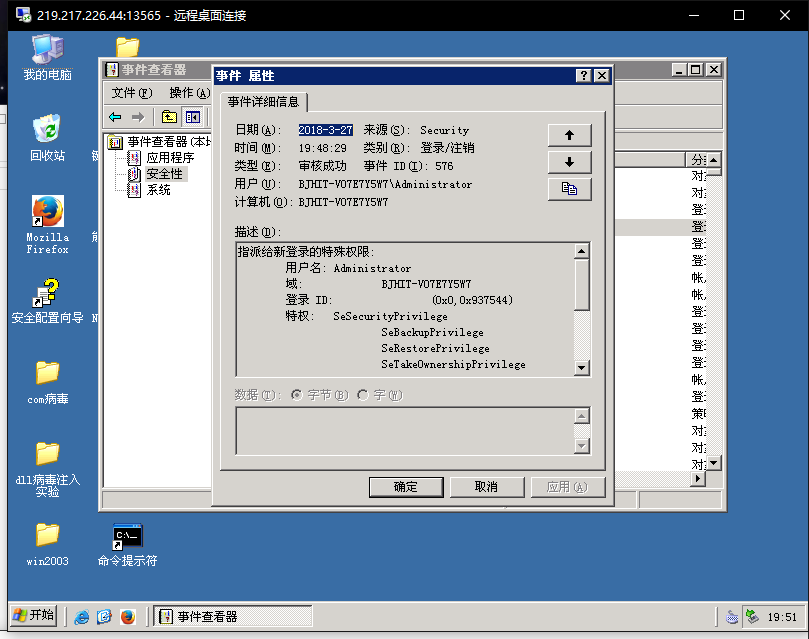


1. 注销当前用户，并重新登录。第一次登录时输入错误密码，第二次输入正确密码，进入系统。





1. 打开“事件查看器”，选择“安全性”，可以看到如下两个事件

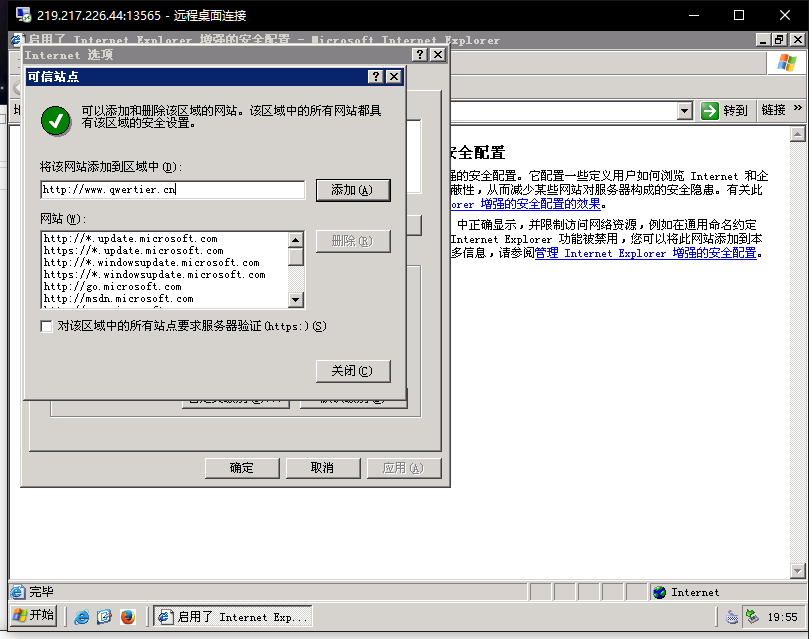




任务五：对 IE 浏览器进行安全配置

1. 在IE“工具”菜单中，选择“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。然后选择不同的区域，点击“自定义级别”，进行自定义设置。

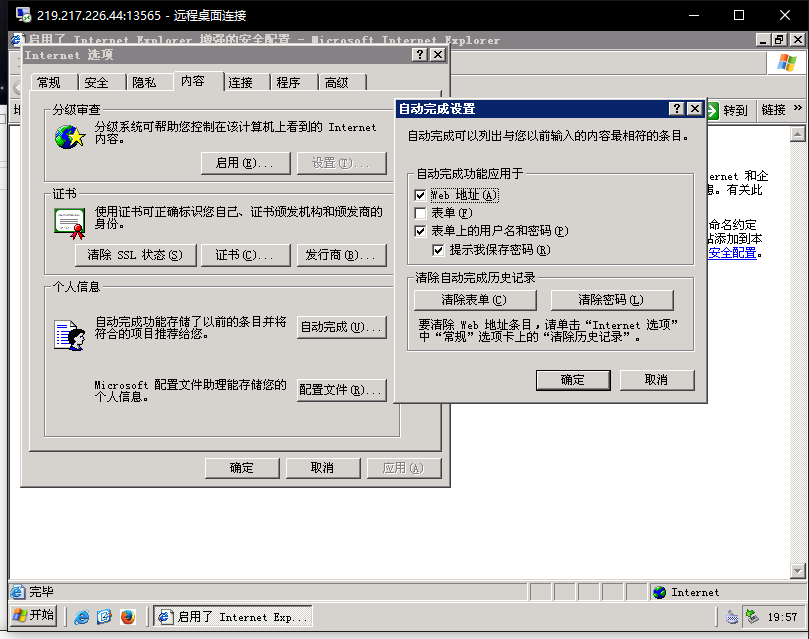




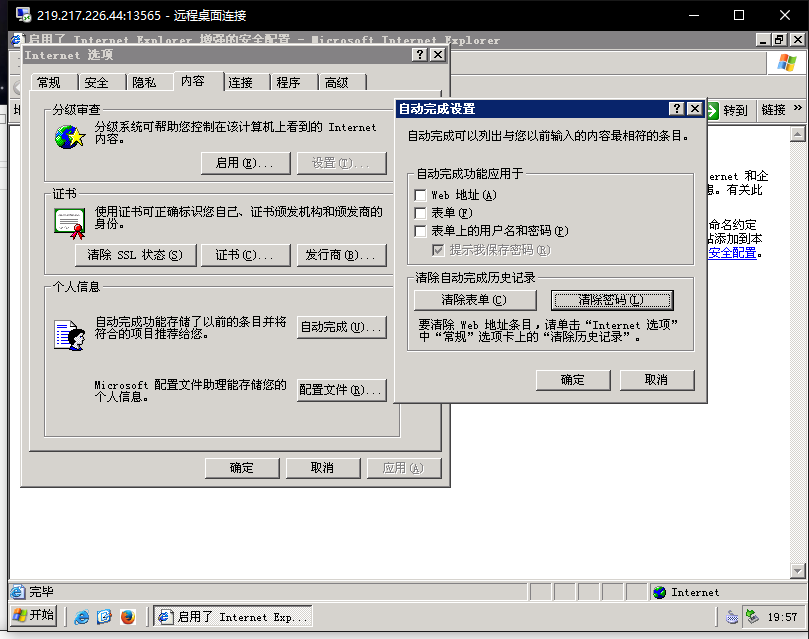




1. 在Internet选项中选择“内容”标签页，点击“自动完成”按钮。

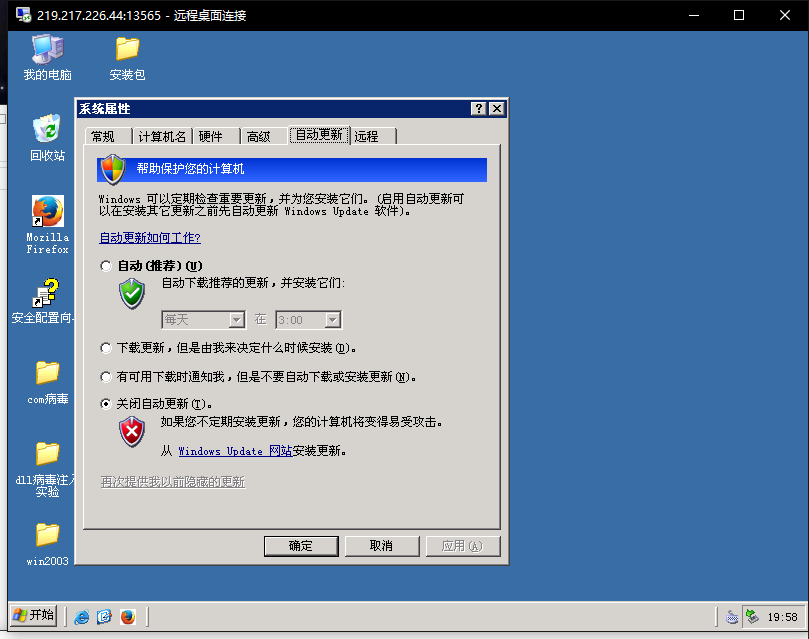


点击“清除表单”和“清除密码”，将上面的自动完成功能都取消。



任务六：对系统补丁自动升级进行配置

1. 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。



选择“自动”并指定自动更新的时间。



五、实验结果总结

*对实验结果进行分析，完成思考题目，总结实验的心得体会，并提出实验的改进意见。*

1. **实验结果分析**
   1. **对Windows 2003系统进行了安全审计策略的配置**
   2. **对Windows 2003系统进行了IE安全策略的配置**
   3. **对Windows 2003系统进行了自动更新策略的配置**
2. **思考题目**
   1. **思考 Windows 中审计管理的作用和意义。**

**通过审计管理，管理员可以对整个系统的动态有更清晰的了解，这不仅能帮助管理员在系统出现功能问题后进行参考，也能帮助管理员在系统出现重大安全问题前及时预防。**

* 1. **详述 Windows 中对账号的审计，及其对登录事件的审计等。**

|  |  |  |  |
| --- | --- | --- | --- |
| **Windows 事件ID** | **Windows Vista 事件 ID** | **事件类型** | **描述** |
| 528, 540 | 4624 | 成功用户登录 | 所有用户登录事件 |
| 529, 530, 531, 532, 533, 534, 535, 536, 537 539 | 4625 | 登录失败 | 所有用户登录失败事件 |
| 538 | 4634 | 成功用户退出 | 所有用户退出事件 |
| 624, 625, 626, 627, 628, 629, 630, 642, 644 | 4720, 4722, 4723, 4724, 4725, 4726, 4738, 4740 | 用户帐号改变 | 用户帐号的改变，像用户帐号创建，删除，改变密码等等 |
| (631 to 641) and (643, 645 to 666) | 4727 to 4737, 4739 to 4762 | 用户组改变 | 对一个用户组的所有改变，例如添加或移除一个全局组或本地组，从全局组或本地添加或移除成员等等 |

**由上表可见，Windows中不同时间ID对应不同类型的事件，而这些事件覆盖了所有与账号有关的事件和与登录有关的事件。**

1. **心得体会**
   1. **通过本次实验，我学到了Windows 2003下安全审核策略的配置方法和配置技巧，并对安全审核的概念和必要性有了进一步的认识。**
   2. **我掌握了Windows 2003下IE浏览器中的安全策略配置**
   3. **我了解了Windows Update的升级策略配置**
2. **改进意见**
   1. **整个实验过程内容非常丰富，但是如果能再加一点对其他配置项（例如复位账户锁定计数器）的简短说明就更好了。**