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： | 马婷婷 |
| 组 号： | 02-34 |
| 实验日期： | 18-03-25 |
| 实验地点： | 远程桌面 |
| 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

**实验设备**： Windows 实验台。

**登录方式：** 远程桌面连接  
**机器名称：** win2003-new

三、实验内容与实验要求

实验内容：

任务一：进行 Windows 操作系统的帐户策略管理

任务二：Windows 操作系统中文件操作的审计策略

任务三：对 Windows 用户账号管理进行审计

任务四：对 Windows 用户登录事件进行审计

任务五：对 IE 浏览器进行安全配置

任务六：对系统补丁自动升级进行配置

实验原理：

运维安全审计系统，即在一个特定的网络环境下，为了保障网络和数据不受来自内部合法用户的不合规操作带来的系统损坏和数据泄露，而运用各种技术手段实时收集和监控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，以便集中报警、记录、分析、处理的一种技术手段。

操作系统的安全配置是整个系统安全审计策略核心，其目的就是从系统根源构筑安全防 护体系，通过用户的一系列设置，形成一整套有效的系统安全策略。

通过建立安全审核策略，使得计算机能够进行下述操作：

1. 跟踪事件的成功和失败。如试图登录、试图建立或修改某个用户帐户或组成员资格、试图访问特定用户指定机密文件、以及试图修改系统的安全设置等。
2. 将未授权访问的风险降至最低。
3. 维护相关用户和系统管理员活动事件的记录。

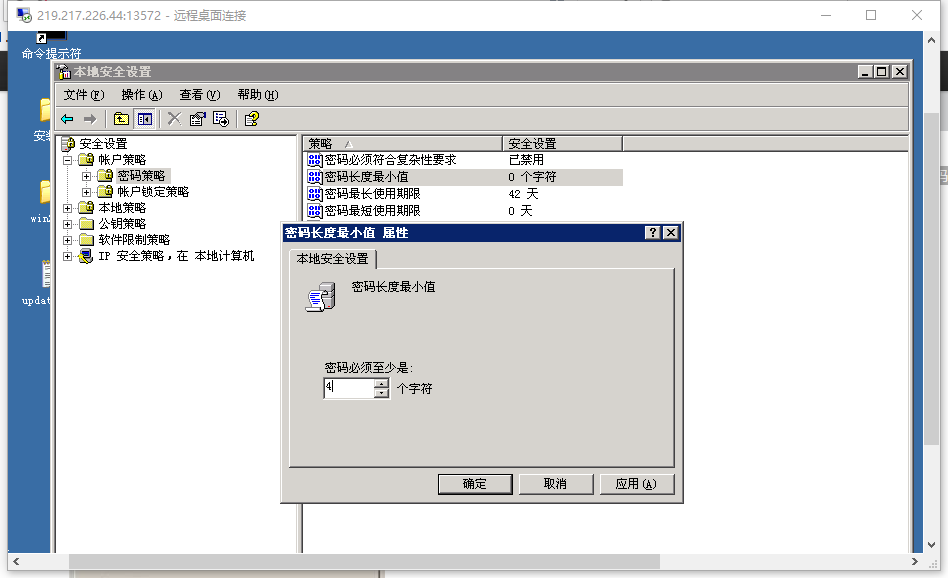
实验要求：

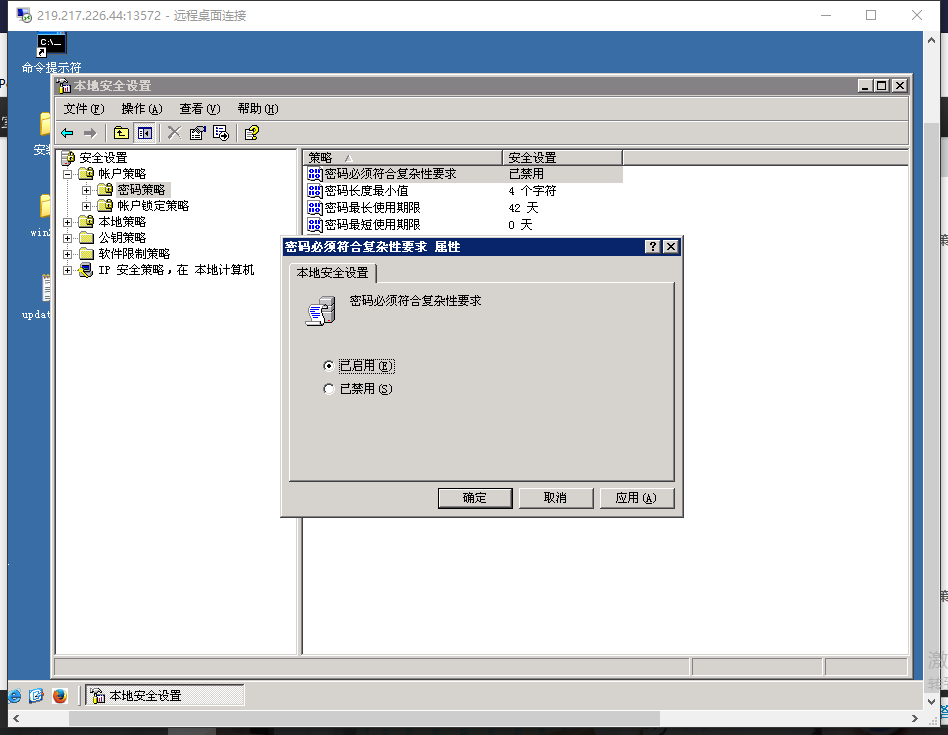
完成以上任务，对实验结果进行分析，完成思考题目，总结实验的心得体会，并提出实验的改进意见。

四、实验过程与分析

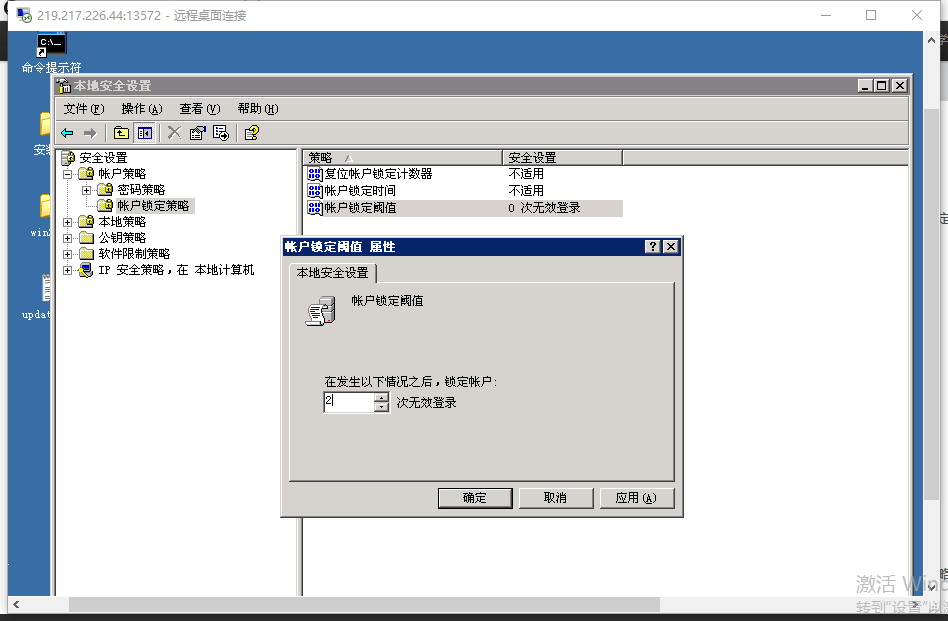
**任务一：**

1. 实验操作者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“帐户策略|密码策略|密码长度最小值”， 通过此窗口设置密码长度的最小值，如下图所示



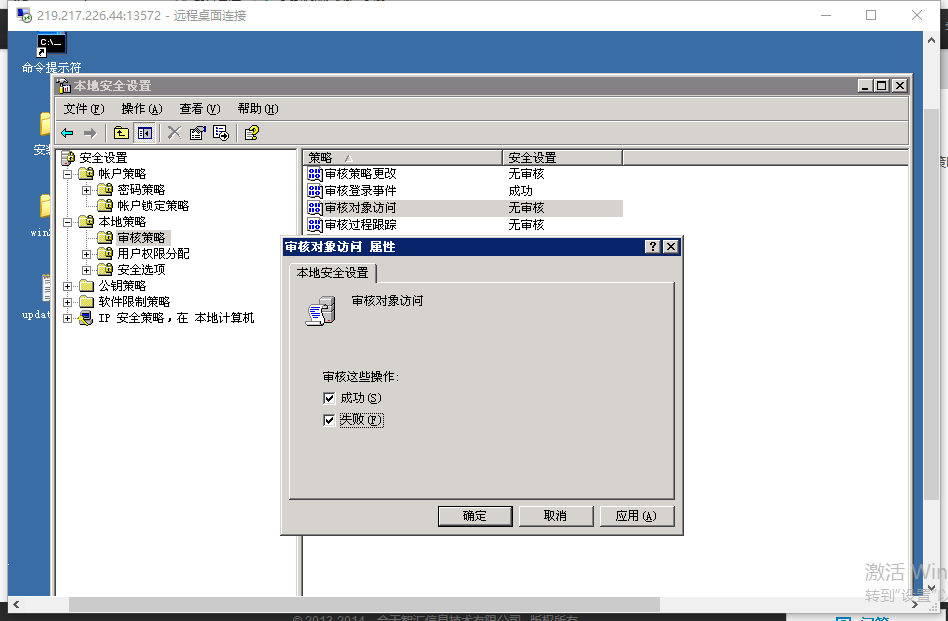


1. 实验操作者以管理员身份登录系统：打开“控制面板|管理工具”，运行“本地安全策 略”；打开“本地安全设置”对话框，选择“帐户策略|帐户锁定策略|帐户锁定阀值”， 如图所示。

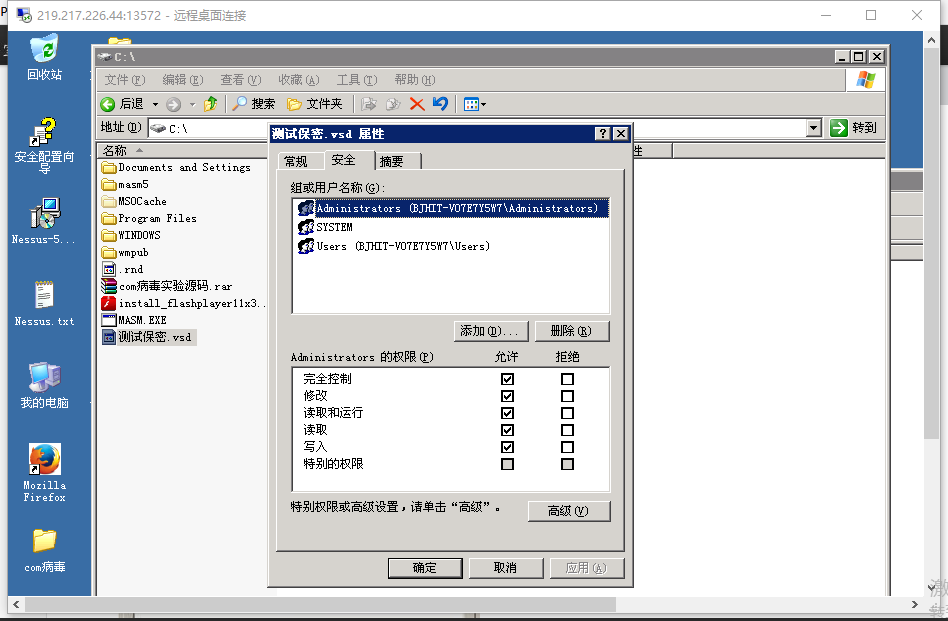


**任务二：**

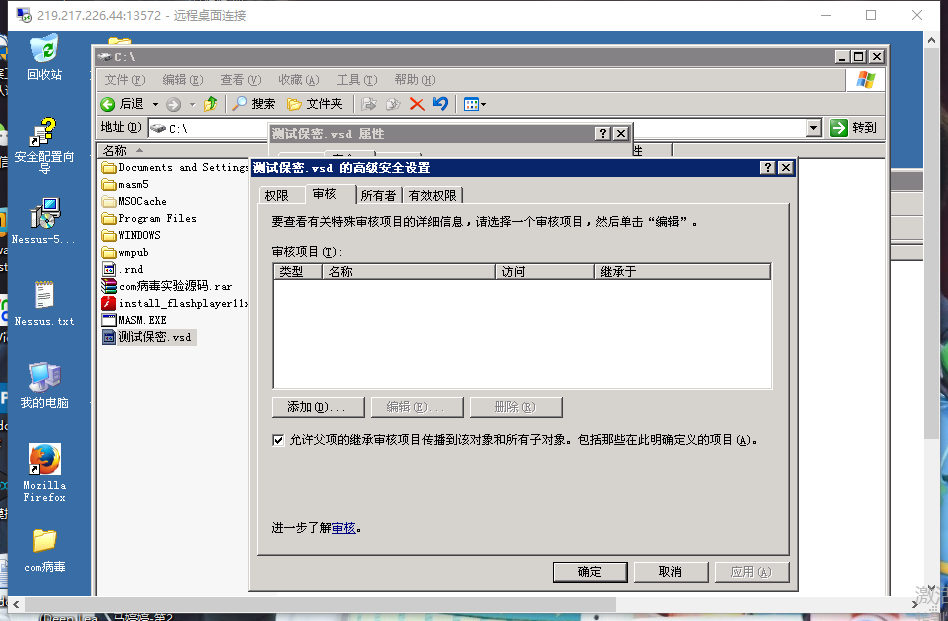
1. 实验操作者以管理员身份登录系统：打开“控制面板|管理工具”，运行“本地安全策 略”；打开“本地安全设置”对话框，选择“本地策略|审核策略”，双击“审核对象 访问”，选“成功”和“失败”，如图所示。



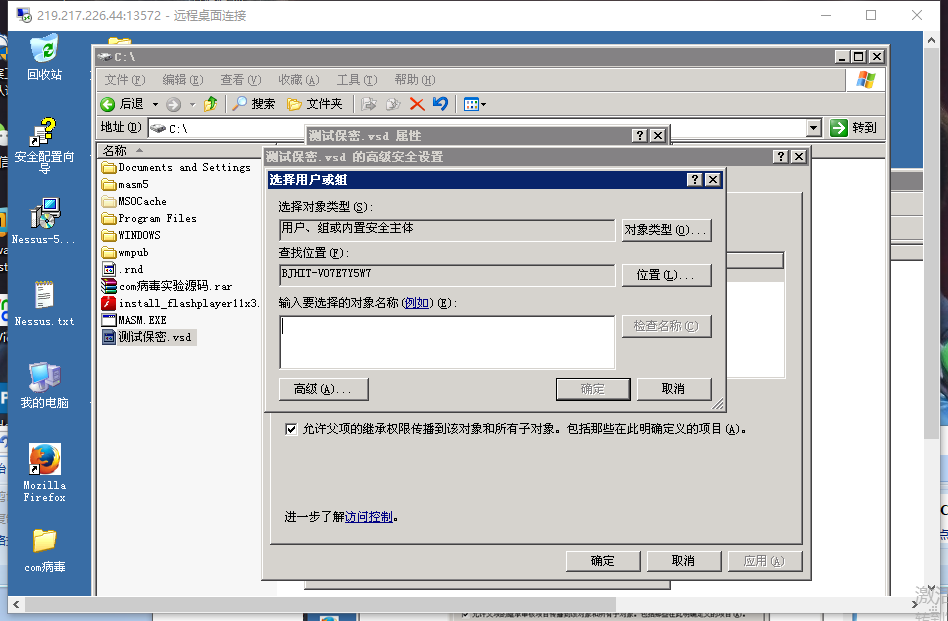
1. 在硬盘上新建一个名为“测试保密.vsd”文件，右键单击该文件，单击“属性”，然后 单击“安全”选项卡。如图所示。



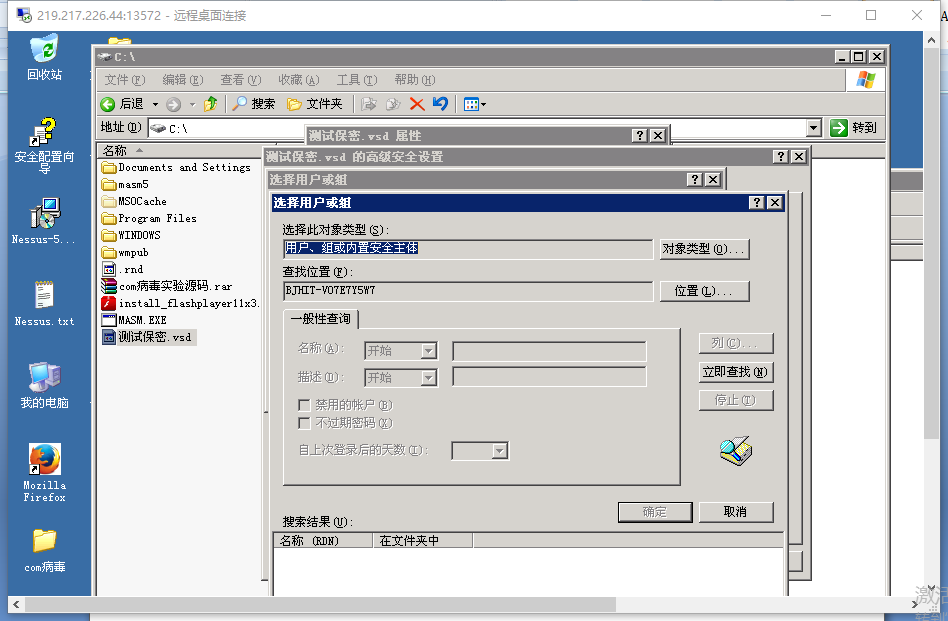
1. 单击“高级”，然后单击“审核”选项卡。如图所示。



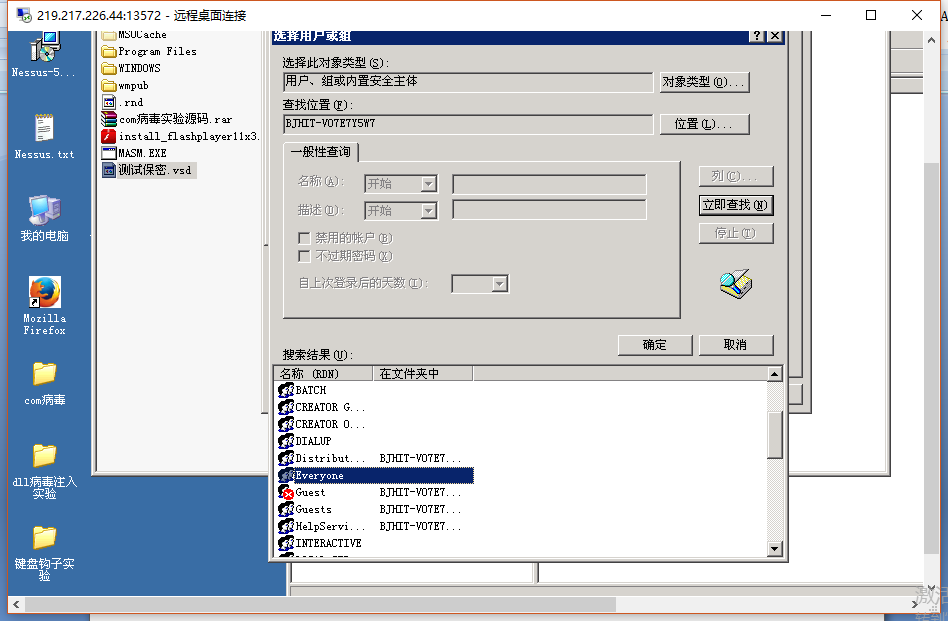
（4）单击“添加”；在“输入要选择的对象名称”中，键入“Everyone”，然后单击“确定”。如图所示

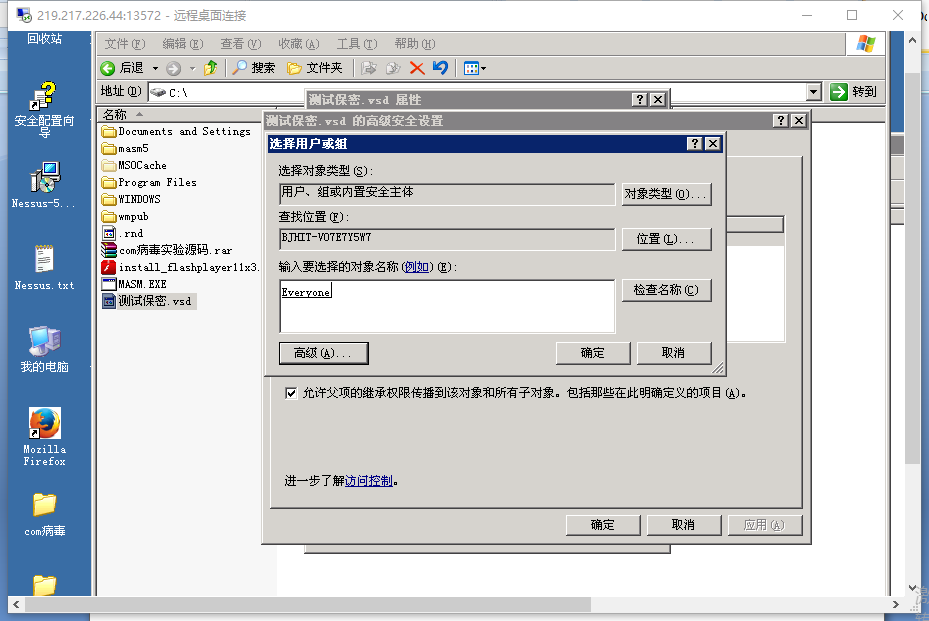


点击高级

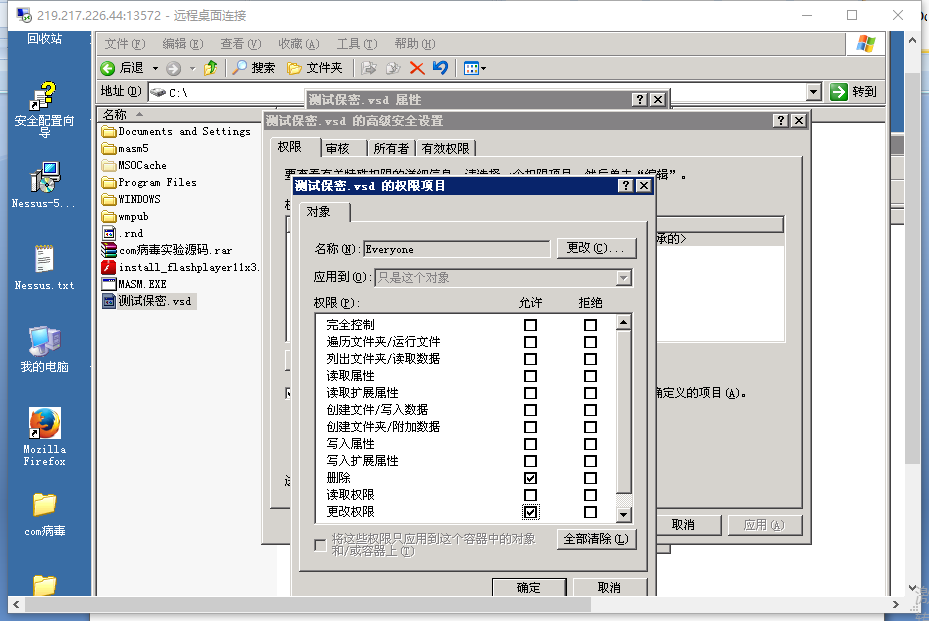


点击立即查找

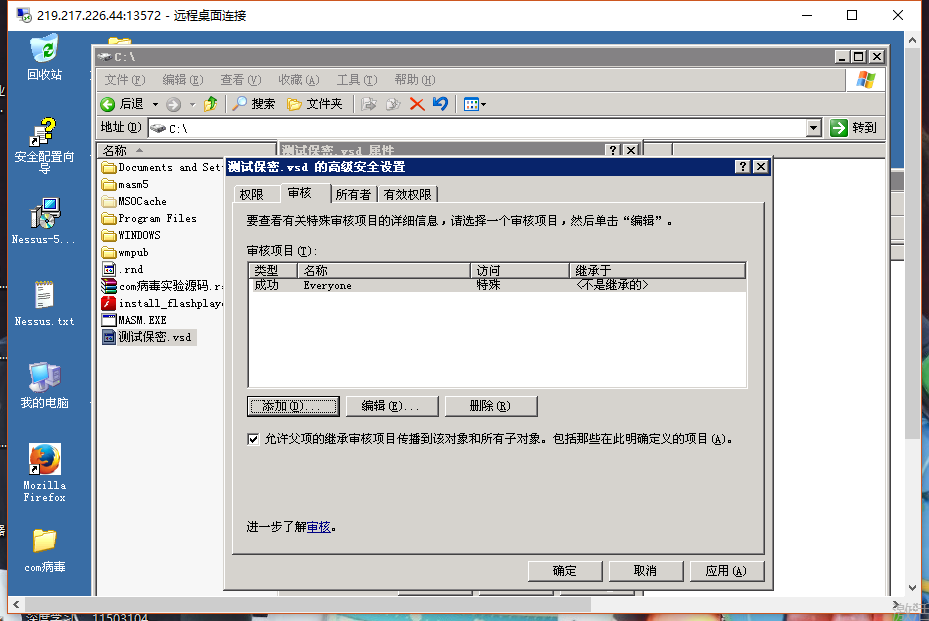
点击确定



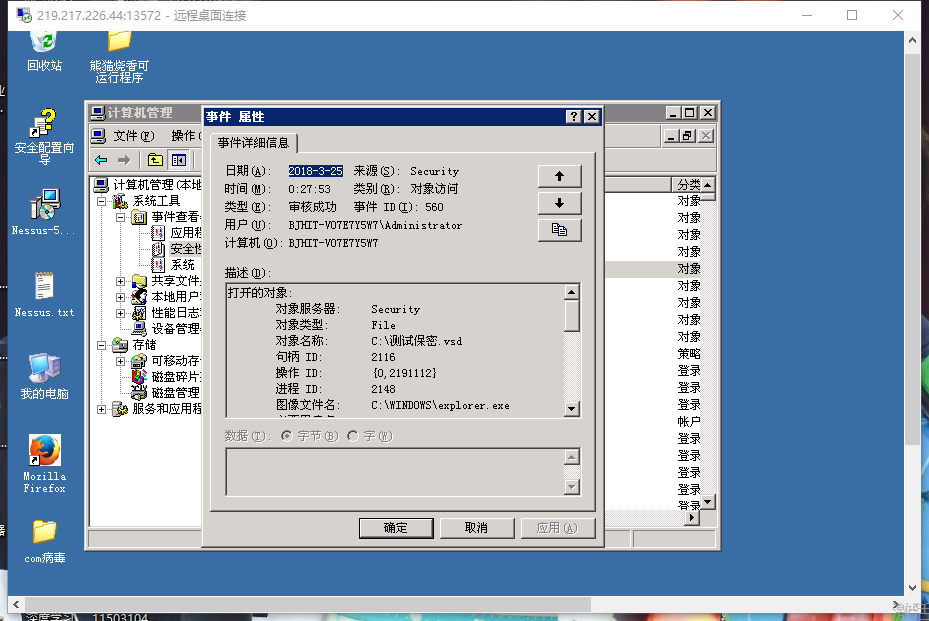
   (5)  在“测试保密.vsd 的审核项目”对话框中，选择访问中的“删除”和“更改权限”的功能；如图所示。



至此，对“测试保密.vsd”的审计设置完后，删除此文件。如图所示。

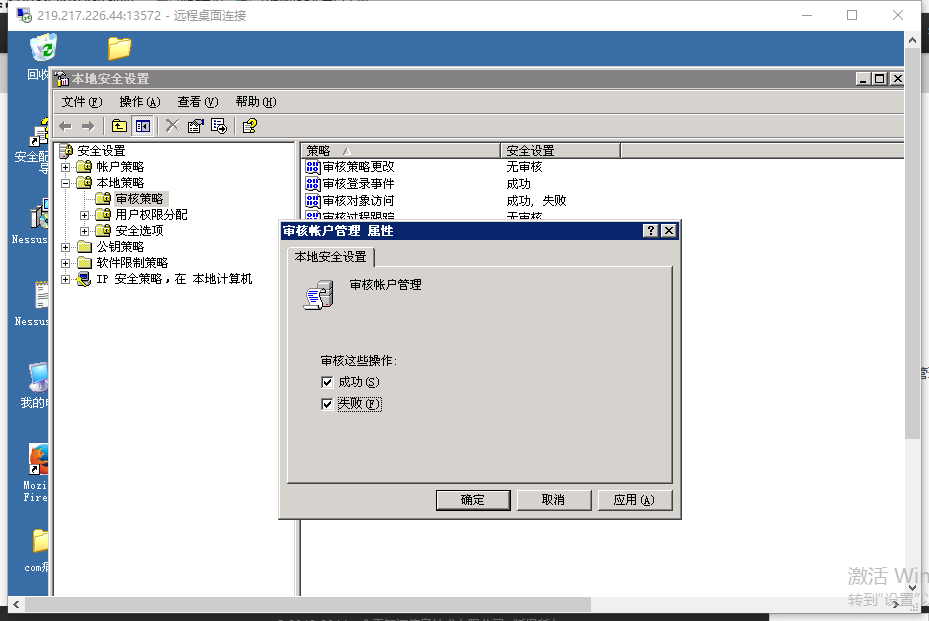


 (6)  右键单击桌面上“我的电脑”，选择“管理”，在计算机管理中，选择“系统工具|事 件查看器|安全性”，或在“开始|运行”中执行  eventvwr.exe，应该能看到。如图所示。

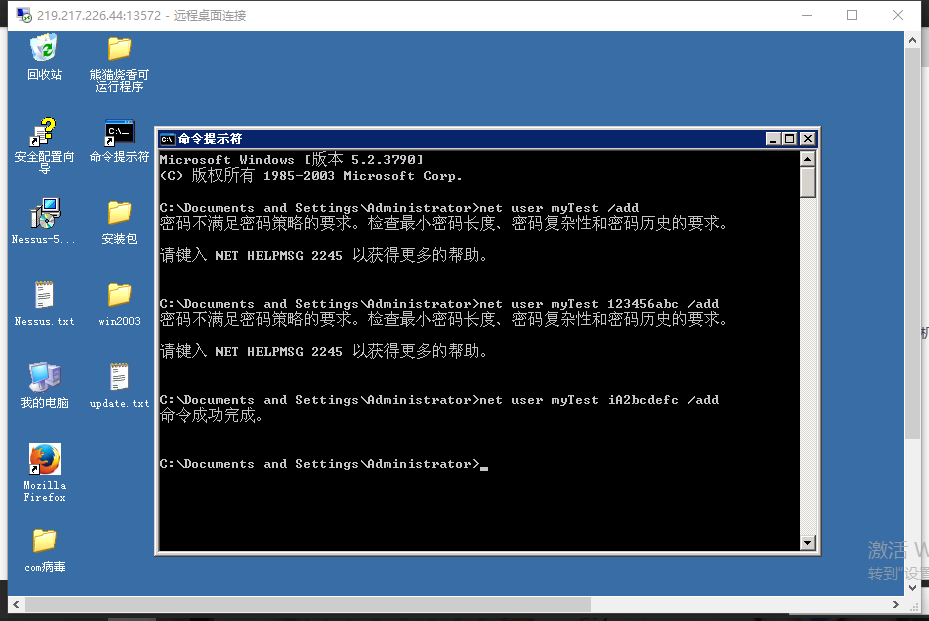


**任务三：对 Windows 用户账号管理进行审计**

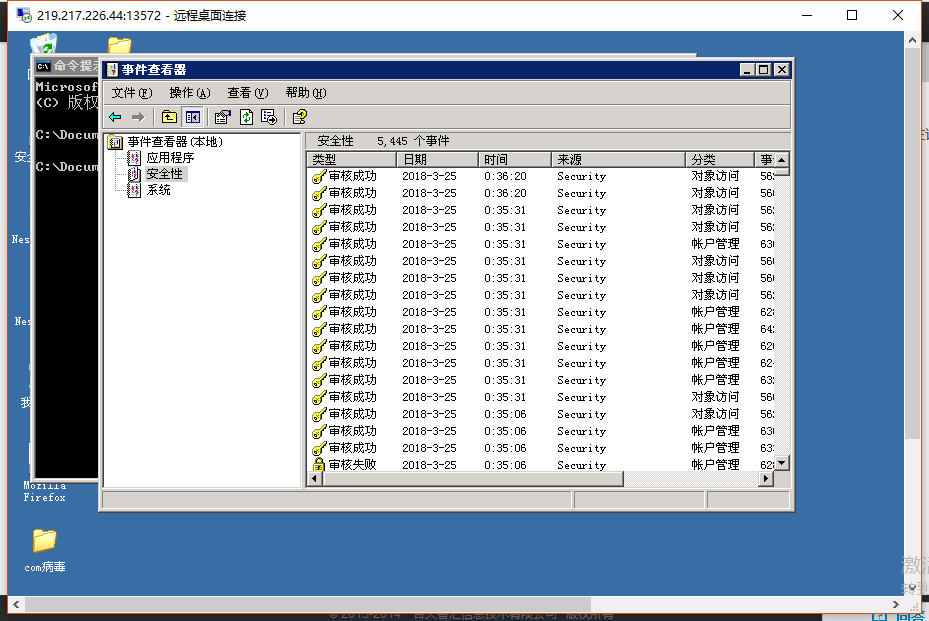
(1)  打开“控制面板|管理工具”，运行“本地安全设置”；选择“安全设置|本地策略|审 核管理”，双击“审核帐户管理”，选“成功”和“失败”。如图所示。



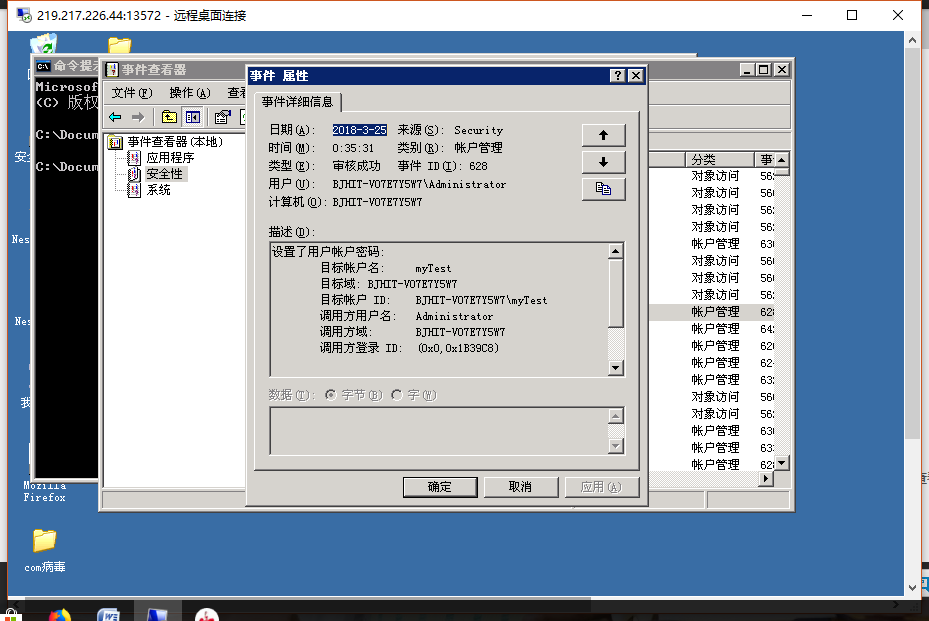
(2)  在“开始|运行”中，输入 cmd，在控制台下输入创建用户 myTest  和设置口令的命令，如图所示。



(3)  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”， 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”，可以看到如图所示的记录：

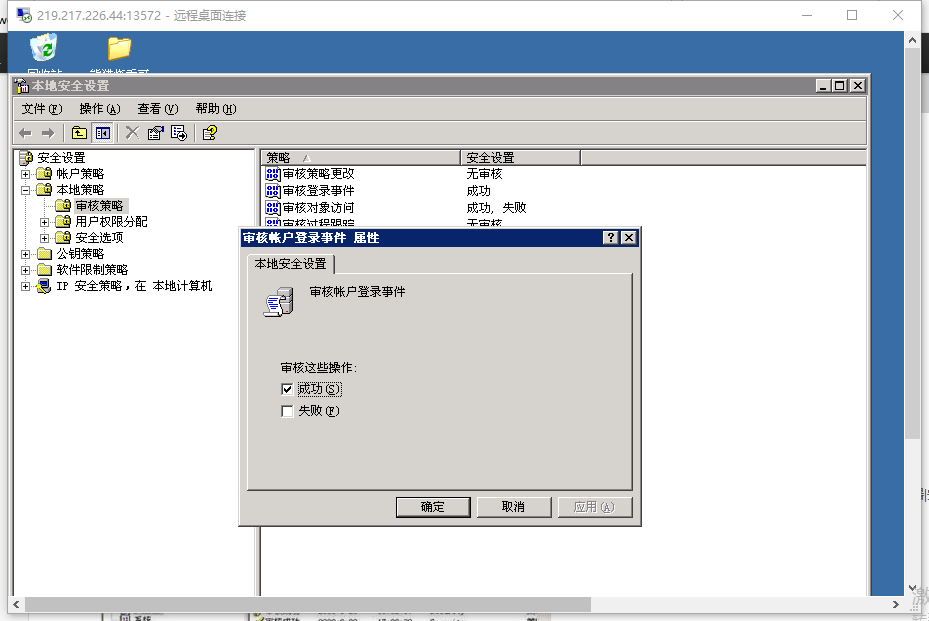


双击审计日志，可以看到如下图所示事件记录

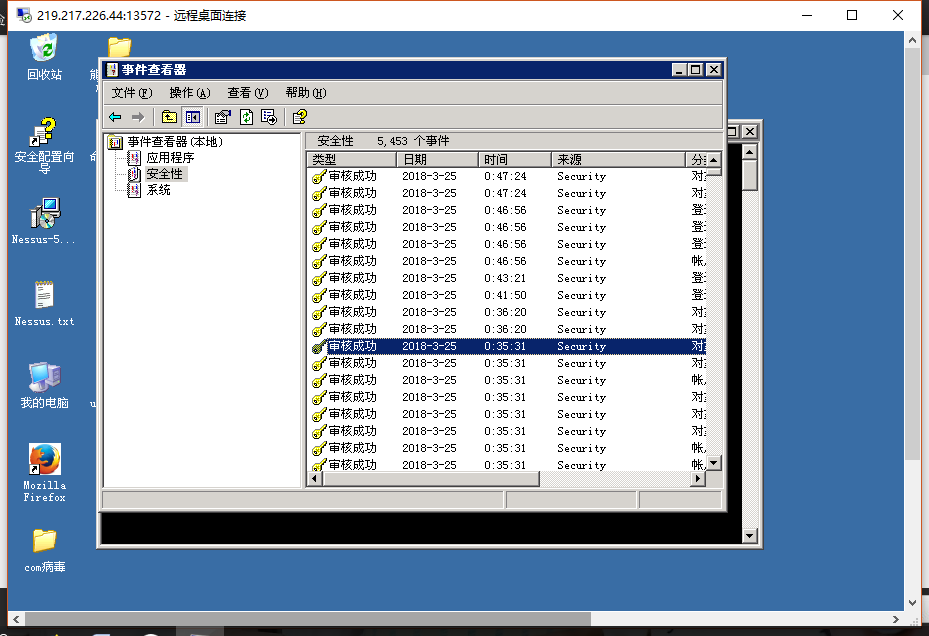


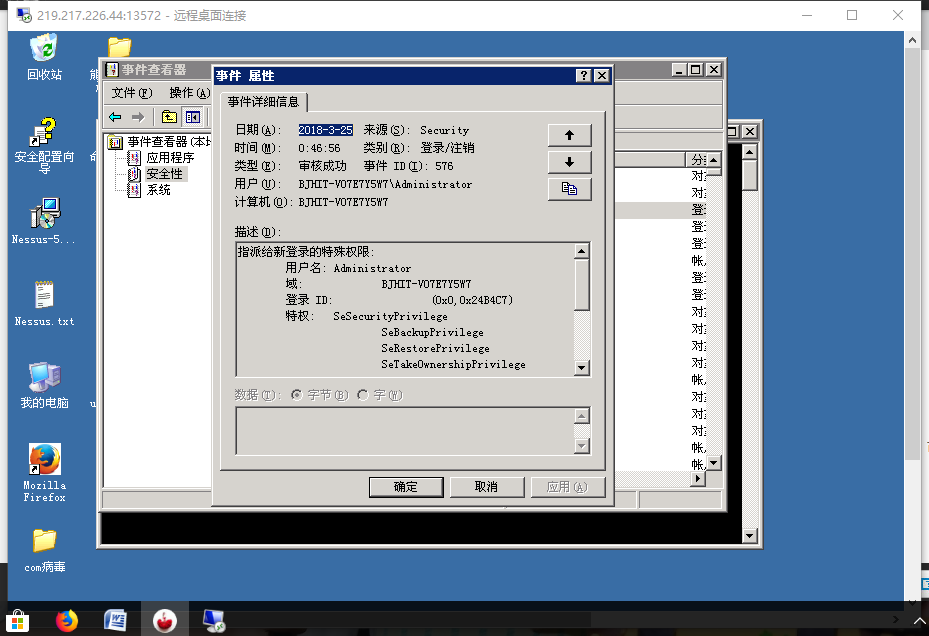
**任务四：对 Windows 用户登录事件进行审计**

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



1. 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。
2. 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”；在打开的“事件查看器” 窗口中选择“安全性”，可以看到如图所示的记录。





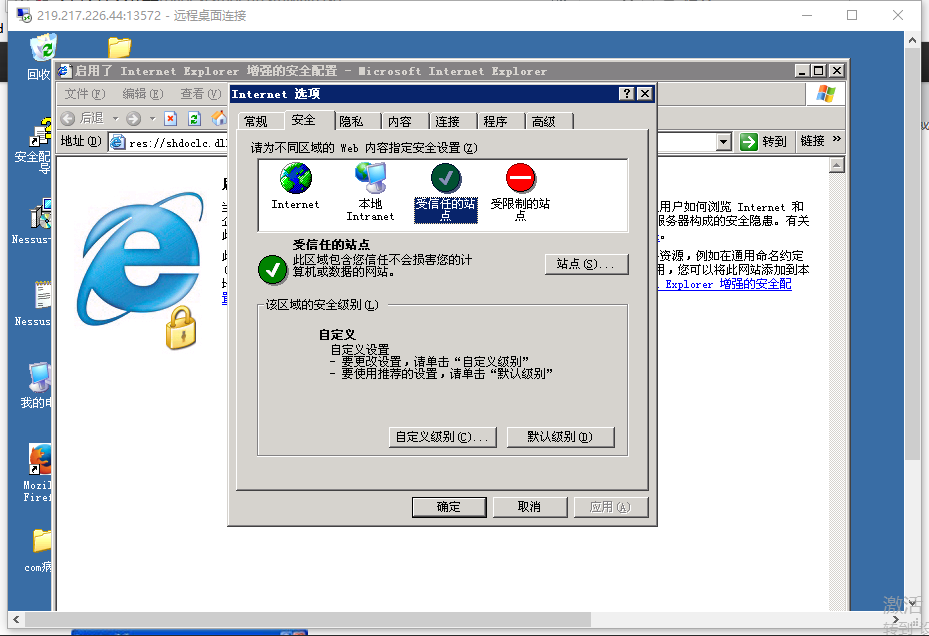


**任务五：对 IE 浏览器进行安全配置**

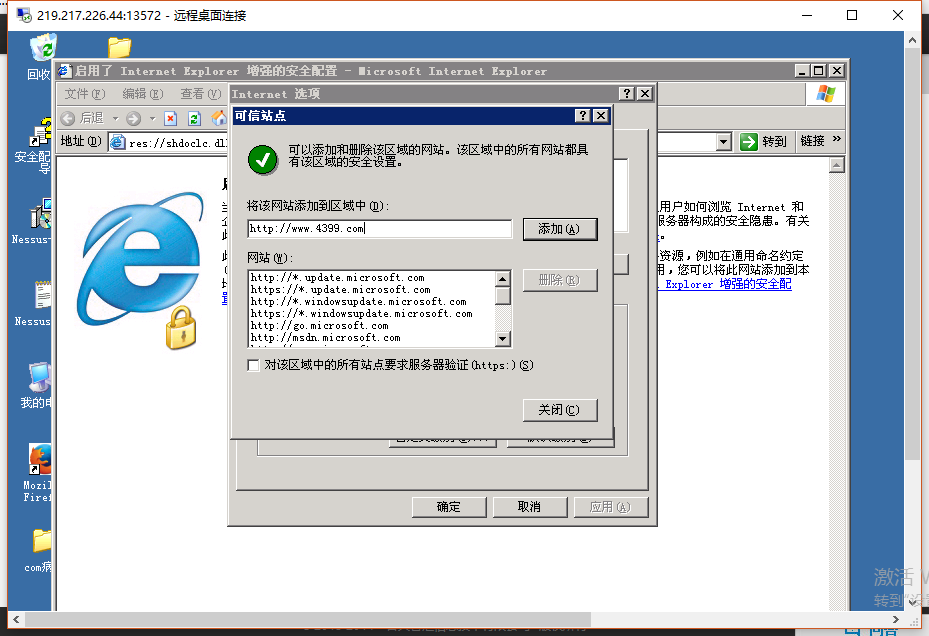
(1)安全区域设置

指定 Web 站点为本地 Intranet 站点、可信站点或受限站点

IE“工具”菜单上，点击“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（默认情况下所有站点都属于 Internet 区域），如图所示。

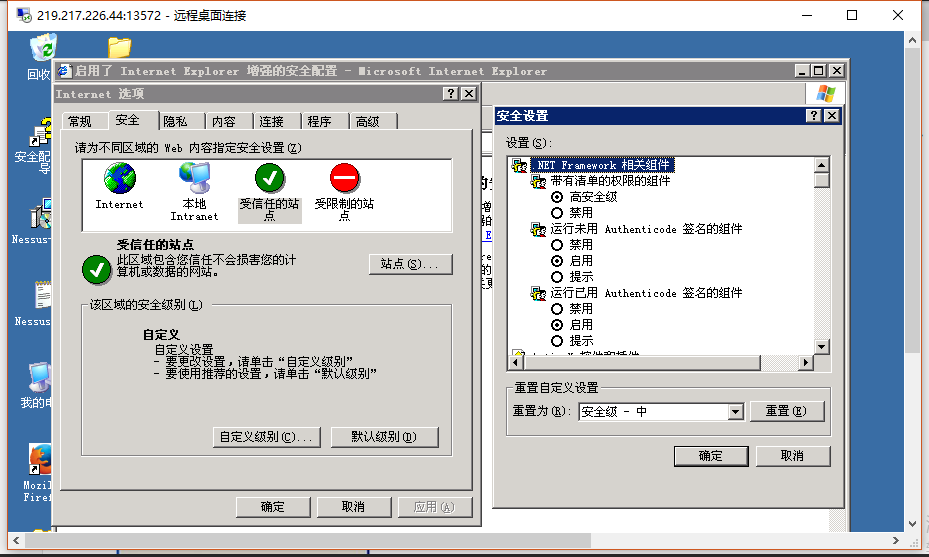


点击“站点”按钮，输入 Web 站点地址点击“添加”按钮，如图所示



改区域的安全级别 在“安全”选项卡上选择要更改其安全级别的区域，点击“自定义级别…”

按钮，进行自定义设置。具体如图所示。

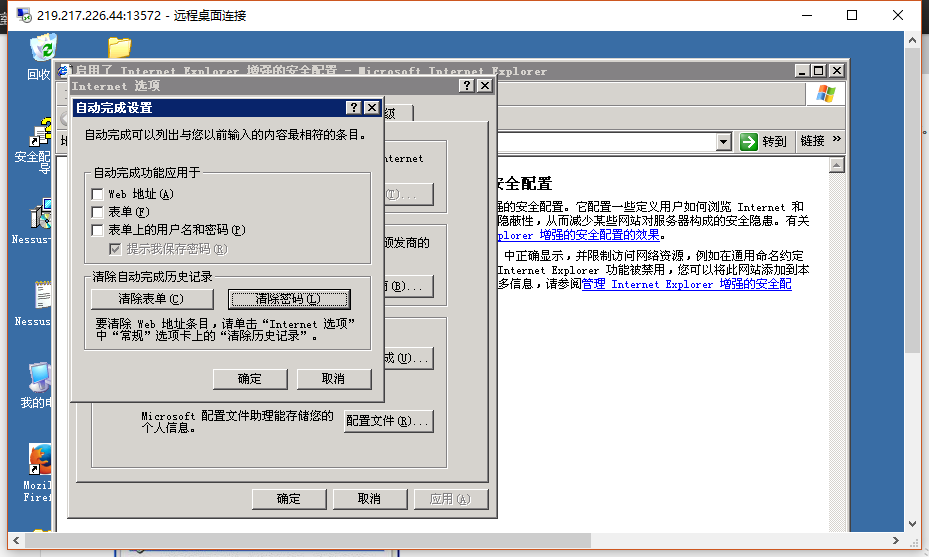


(2)自动完成配置

IE 浏览器默认打开自动完成功能，在 Internet 选项中选择“内容“标签页，点击“自动完成”按钮，如图所示。

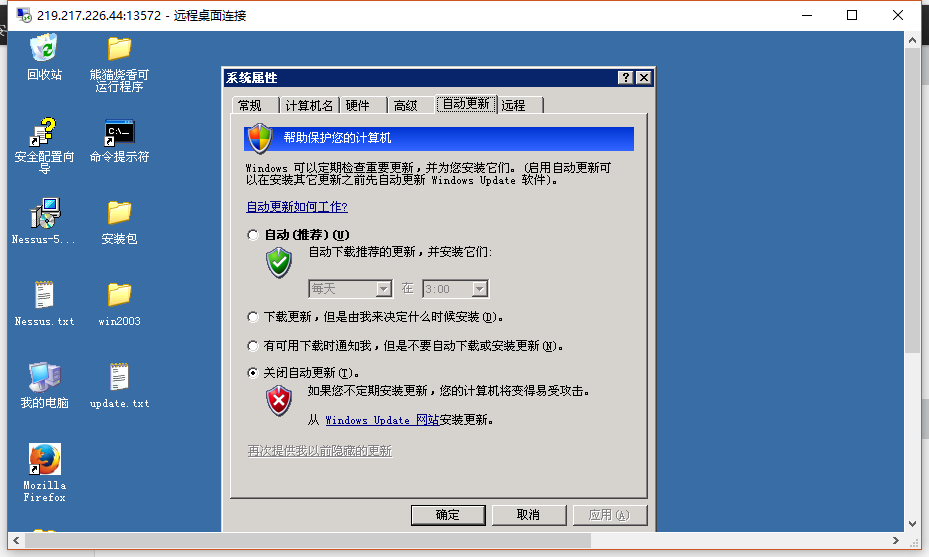


在弹出的“自动完成设置”窗口中点击“清除表单”和“清楚密码”按钮，也可以取消上方复选框的选择以停用自动完成功能，如图所示

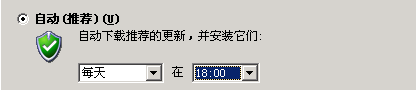


**任务六：对系统补丁自动升级进行配置**

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，如图所示



选择“自动“并指定自动更新的时间，如图 所示，系统会按时自动进行补丁升级。



**实验中遇到的问题以及解决方案：**

任务三在进行账户创建的时候运行“net user myTest /add”出现错误提示：“密码不满足密码策略的要求。检查最小密码长度、密码复杂性和密码历史的要求。”这是由于任务一对于密码长度和密码复杂性做了设置，比如最小长度不能小于4，复杂性要求等等。通过设置较为复杂的密码，运行“net user myTest 密码 /add”命令成功创建账户。

五、实验结果总结

**思考问题：**

1. 思考 Windows 中审计管理的作用和意义。

操作系统的安全配置是整个系统安全审计策略核心，其目的就是从系统根源构筑安全防 护体系，通过用户的一系列设置，形成一整套有效的系统安全策略。

通过建立安全审核策略，使得计算机能够进行下述操作：

1.跟踪事件的成功和失败。如试图登录、试图建立或修改某个用户帐户或组成员资格、试图访问特定用户指定机密文件、以及试图修改系统的安全设置等。

2.将未授权访问的风险降至最低。

3.维护相关用户和系统管理员活动事件的记录。

2）详述 Windows 中对账号的审计，及其对登录事件的审计等。

Windows中可以对用户的账号管理审计、账户策略管理审计。需要在本地安全策略中配置“账户策略”或者“审核账户管理”等选项，来对密码长度、密码复杂性，以及创建、删除、更改账户等方面审计。当一个用户账户或者安全组被创建、更改或者删除时，账户管理事件发生，或者当一个用户账户改名、启用或者失效，设置或更改密码时，账户管理时间发生。审核账户管理是基于“成功”和“失败”两种情况的。根据相应的配置，成功创建账户等行为会在“事件查看器”中都可以看到相应的记录。

Windows也可以对账号登录事件审计。审核失败登录企图，它可以用来指示有人试图用不同的错误密码登录。如果关心有人用偷来的密码登录，那么审核成功登录的时间。当一个用户试图通过网络登录或者退出，并验证到一个本地用户账户时，账户登录事件发生。我们可以在本地安全设置里，对“审核账户登录事件”进行“成功”或者“失败”的配置，来达到我们想要的审核效果，相应的日志也在“事件查看器”的安全性中可以看到。

**心得体会：**

通过本次实验我学习了Windows 2003 中安全审计策略的配置，自己动手操作了Windows 2003中对于账户审计、文件操作审计、账户管理、用户登录事件等方面的审计策略的配置，查看了相应的时间记录，进一步理解了 Windows 2003 中审计策略的作用，从系统根源构筑安全防护体系，通过用户的一系列设置，形成一整套有效的系统安全策略。除此之外，我还掌握 IE 浏览器的安全策略配置，以及手动对系统补丁的升级策略进行合适的配置。提高了动手操作的能力，进一步理解了审计策略配置对于我们系统安全的重要性。

**改进意见：**

本次实验的操作较为简单，在之前对账户审计的配置有可能会影响到添加用户时候，对于密码复杂性的要求，但是通过助教给的word已经说明了这个问题。因此这次实验感觉还是很完备的。