哈尔滨工业大学计算机学院

《windows审计策略》

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： | 韩越 |
| 组 号： | 第二组11号 |
| 实验日期： | 2018-03-26 |
| 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。 Windows server 2003。

网络拓扑见下图：



三、实验内容与实验要求

准备工作

打开 Windows 实验台，运行 Windows 2003 系统。

任务一：进行 Windows 操作系统的帐户策略管理

设置账户相关的密码、锁定账户等安全策略。

任务二：Windows 操作系统中文件操作的审计策略

开启审核对象访问，记录文件操作。

任务三：对 Windows 用户账号管理进行审计

对账号管理（如添加账号）进行审计和记录。

任务四：对 Windows 用户登录事件进行审计

记录用户登录（成功或失败）。

任务五：对 IE 浏览器进行安全配置

配置IE浏览器的安全等级等设置

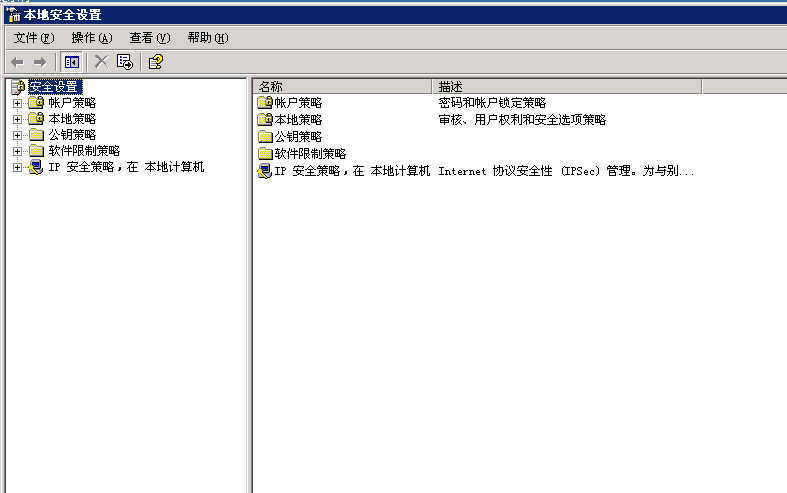
任务六：对系统补丁自动升级进行配置

设置自动升级和补丁计划

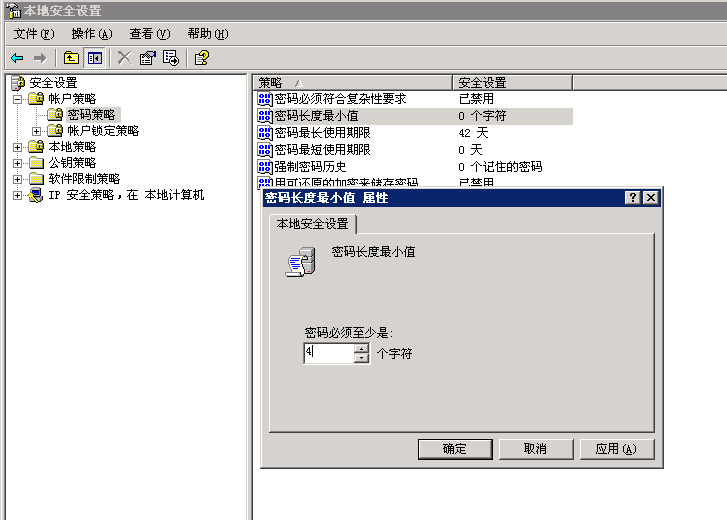
四、实验过程与分析

**任务一：进行 Windows 操作系统的帐户策略管理**

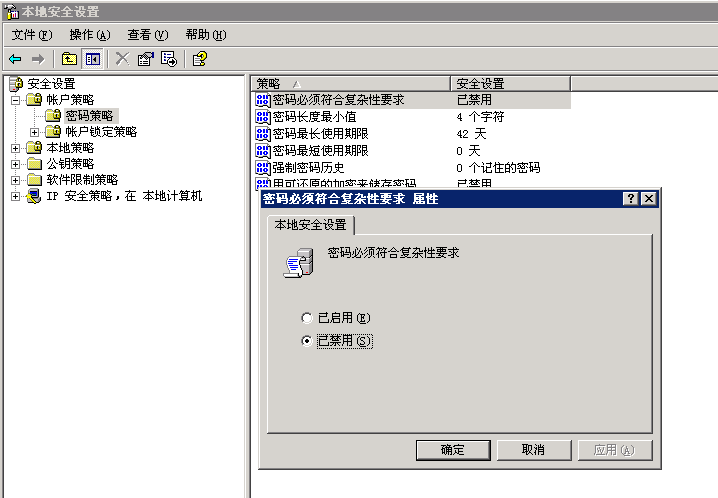
(1) 实验操作者以管理员身份登录系统：打开“控制面板|管理工具”，运行“本地安全策 略”。



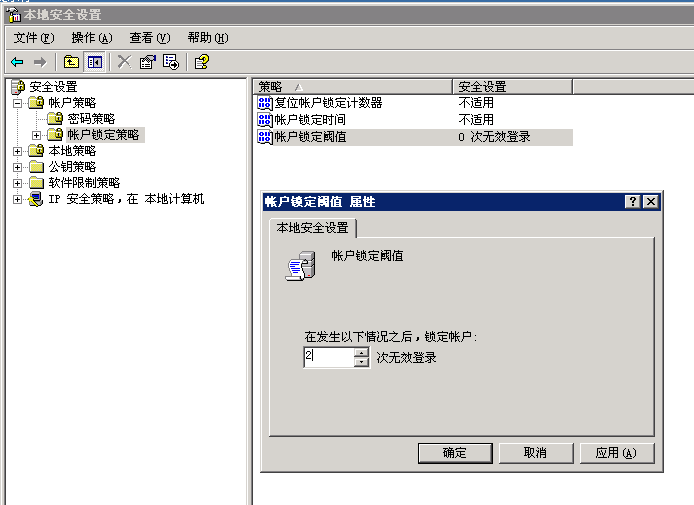
打开“本地安全设置”对话框，选择“帐户策略|密码策略|密码长度最小值”， 通过此窗口设置密码长度的最小值。



选择“密码必须符合复杂性要求”，通过此窗口可以启用此功能。

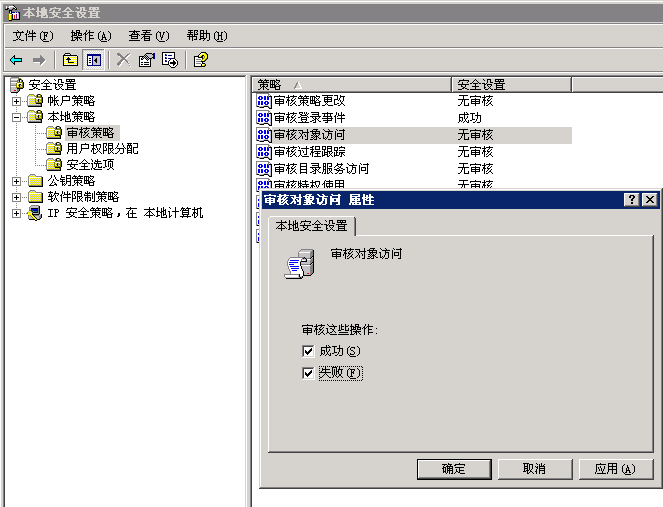


(2) 选择“帐户策略|帐户锁定策略|帐户锁定阀值”

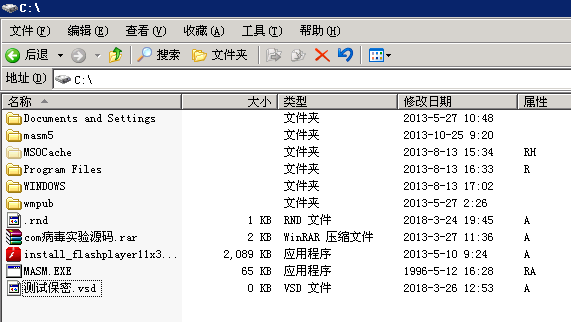


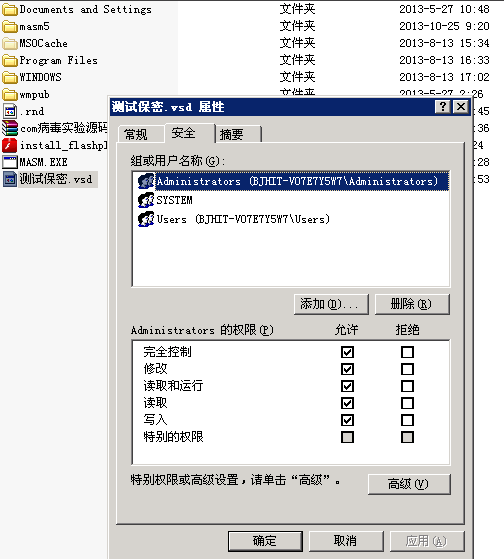
# 任务二：Windows 操作系统中文件操作的审计策略

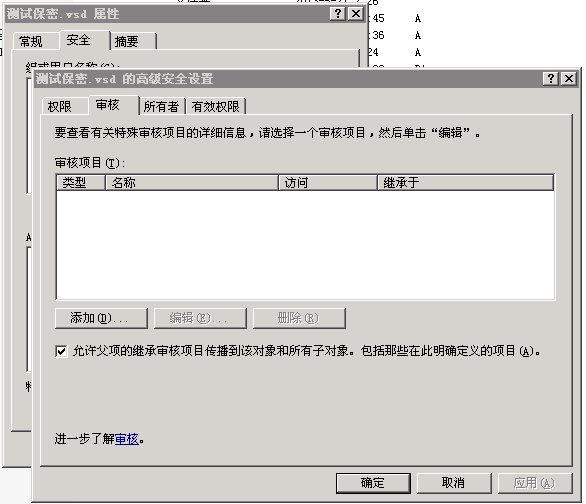
 (1) 选择“本地策略|审核策略”，双击“审核对象 访问”，选“成功”和“失败”



(2) 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。

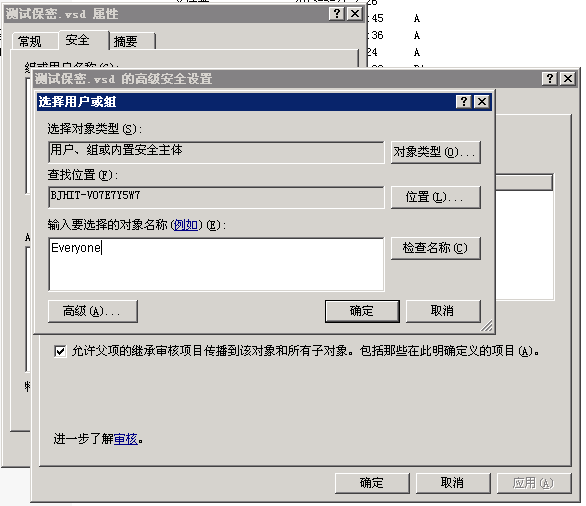


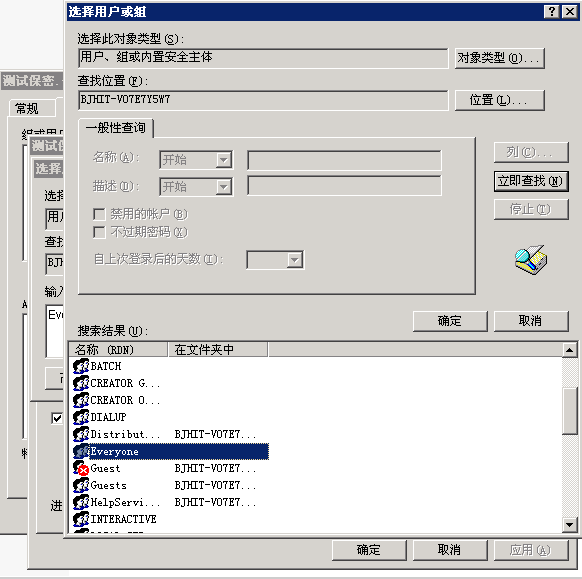


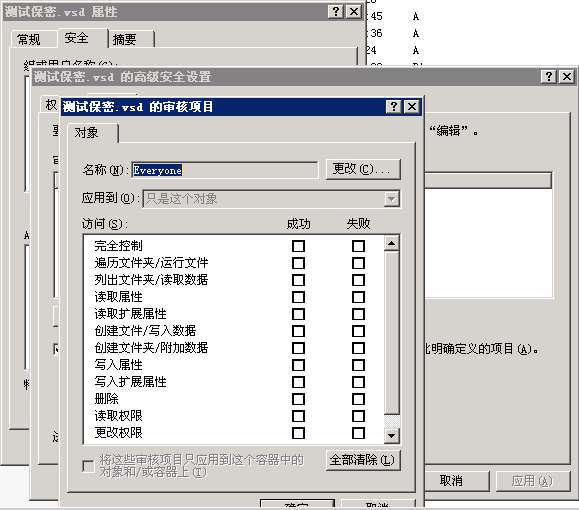
(3) 单击“高级”，然后单击“审核”选项卡。如图所示。

(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”。

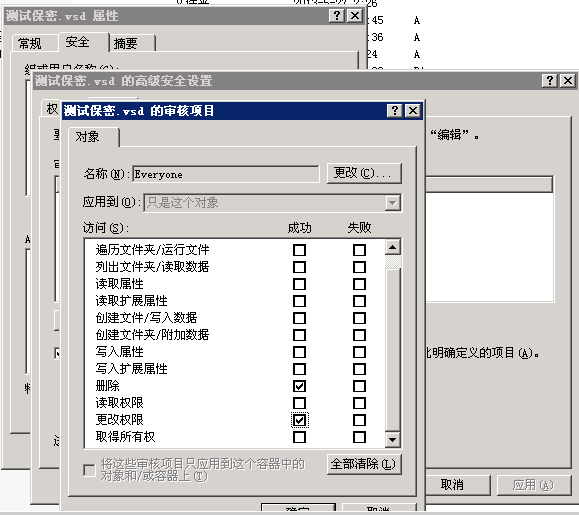
实际上不是自己输Everyone，只需去高级里面查找就行。



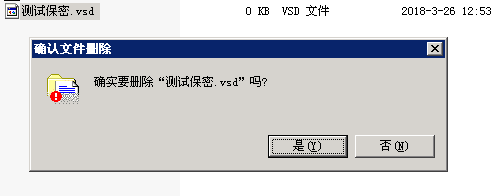




  (5)  在“测试保密.vsd 的审核项目”对话框中，选择访问中的“删除”和“更改权限”的功能



 至此，对“测试保密.vsd”的审计设置完后，删除此文件。

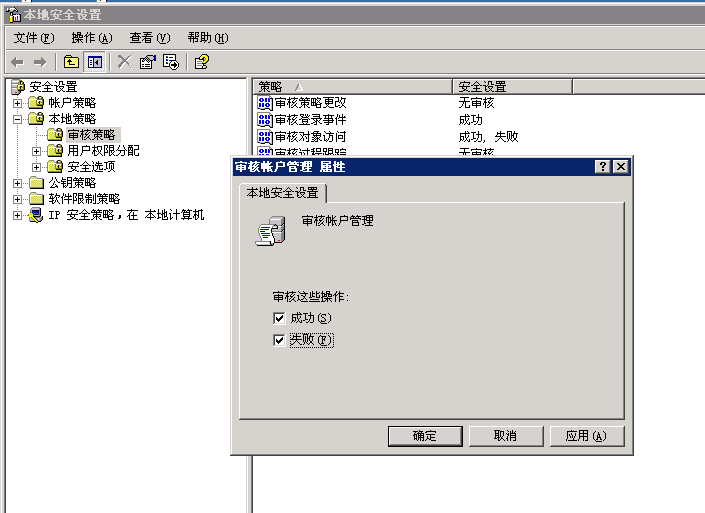


 (6)  右键单击桌面上“我的电脑”，选择“管理”，在计算机管理中，选择“系统工具|事 件查看器|安全性”。 可以看到如图所示的记录

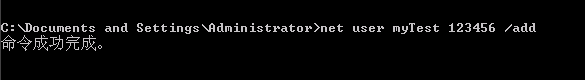


# 任务三：对 Windows 用户账号管理进行审计

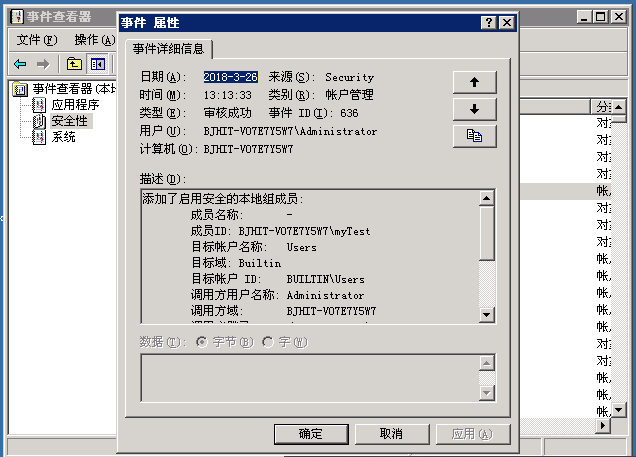
(1) 打开“控制面板|管理工具”，运行“本地安全设置”；选择“安全设置|本地策略|审 核管理”，双击“审核帐户管理”，选“成功”和“失败”。



(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。

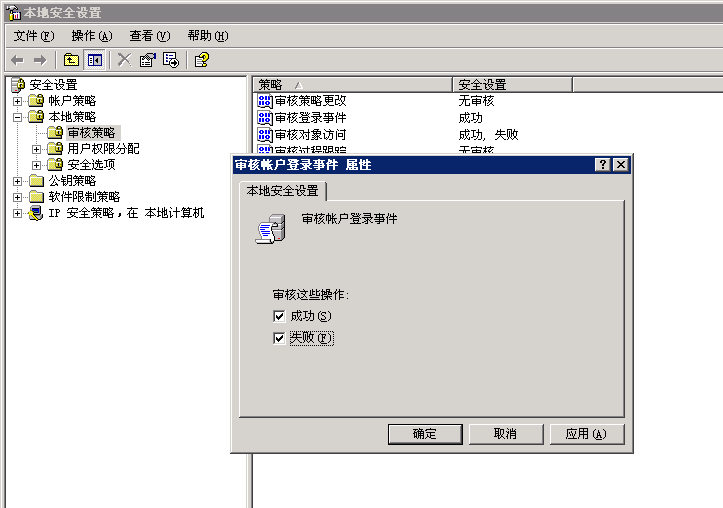


(3) 在“开始|运行”中执行 eventvwr.exe，在打开的“事件查看器”窗口中选择“安全性”， 或右键单击桌面上“我的电脑”，选择“管理”，在计算机管理中，选择“系统工具| 事件查看器|安全性”，可以看到如图所示的记录。



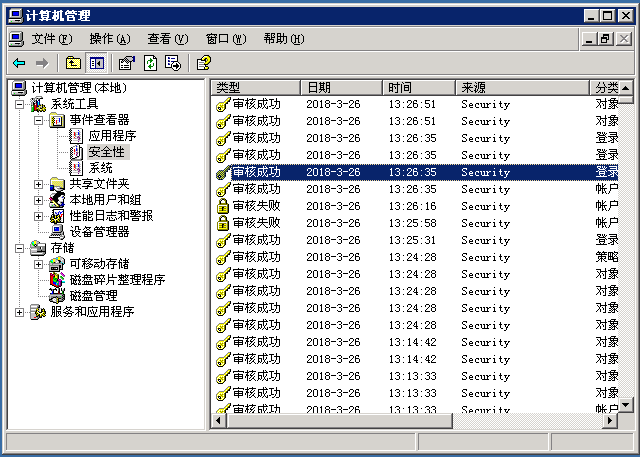
# 任务四：对 Windows 用户登录事件进行审计

(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”。

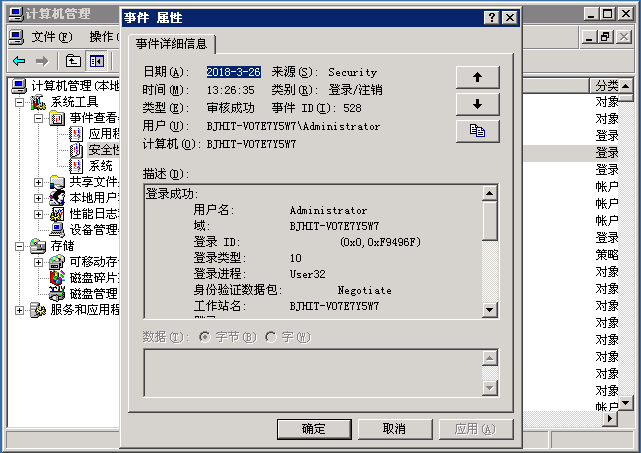


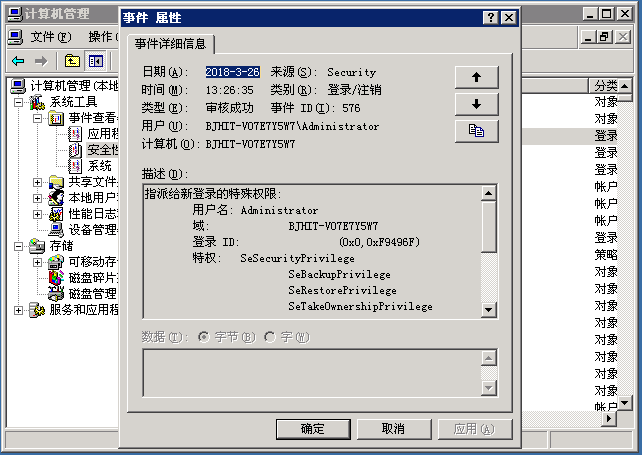
(2) 注销当前用户，并能从新登录，登录输入密码是第一次输错密码，第二次输入正确密码，进入系统。

(3) 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。



(4) 双击审计日志，应可以看到如下两图所示的事件记录。





# 任务五：对 IE 浏览器进行安全配置

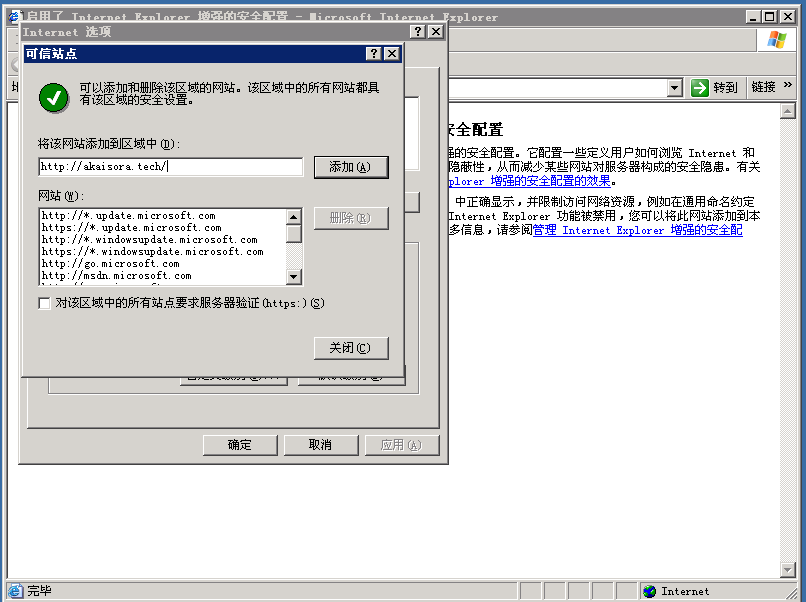
(1)安全区域设置

指定 Web 站点为本地 Intranet 站点、可信站点或受限站点

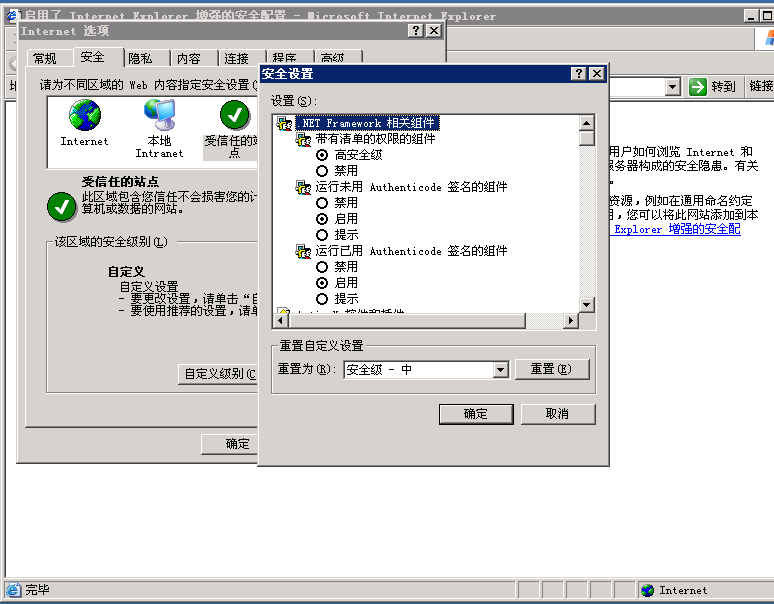
在 IE“工具”菜单上，点击“Internet 选项”，选择“安全”选项卡，然后选择将要把 Web 站点指定到的安全区域：本地 Intranet、可信站点或受限站点（默认情况下所有站点都属于 Internet 区域），如图所示。



 点击“站点”按钮，输入 Web 站点地址点击“添加”按钮，如图所示。

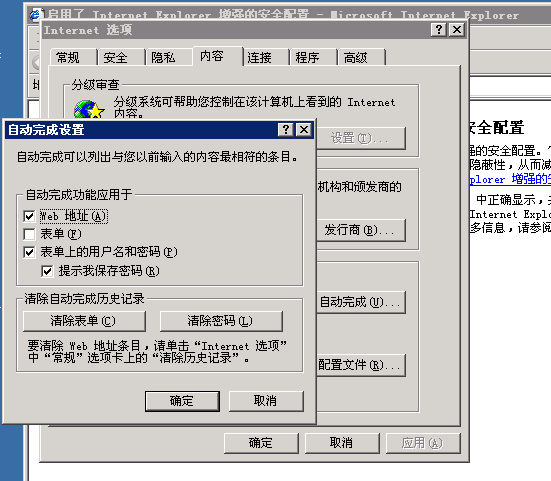


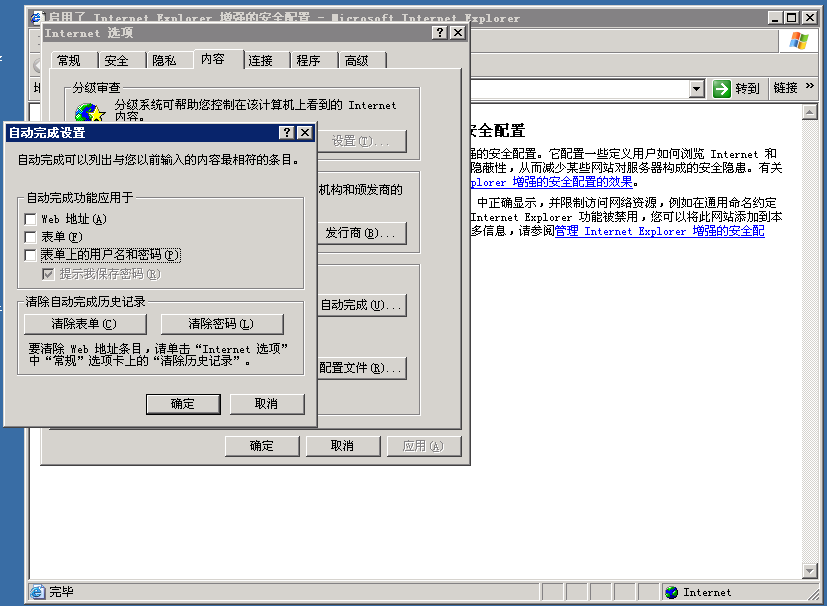
改区域的安全级别 在“安全”选项卡上选择要更改其安全级别的区域，点击“自定义级别…”按钮，进行自定义设置。具体如图所示。



(2)自动完成配置

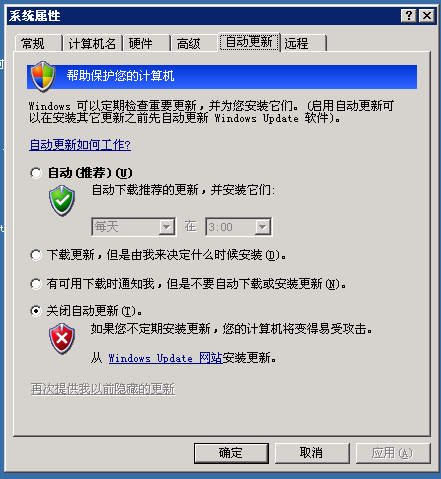
IE 浏览器默认打开自动完成功能，在 Internet 选项中选择“内容“标签页，点击“自动完成”按钮，如图所示。



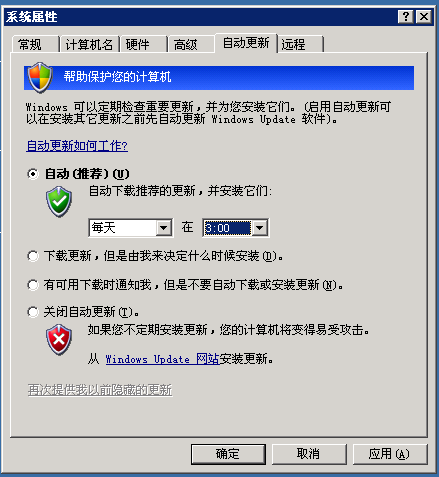


# 任务六：对系统补丁自动升级进行配置

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 1.1-68 所示，系统会按时自动进行补丁升级。



五、实验结果总结

**实验结果分析**

学习了Windows审计策略和安全功能的使用方法，以及事件查看器的事件查看方法。

成功地对windows中账户、文件、账户管理、登录等操作配置审计策略和事件查看，在事件管理其中看到了我们创建账户myTest的记录，账户登录成功和失败记录以及对“测试保密.vsd”文件的删除记录。

成功对Internet选项中安全等级等设置进行配置。成功对window自动更新计划进行了设置。

**思考题**

1）思考 Windows 中审计管理的作用和意义。

用来记录用户操作过程中某些行为的记录。审计管理每当用户执行了指定的某些操作，审核日志就会记录一个审核项。例如，修改文件或策略可以触发一个审核项。审核项显示了所执行的操作、相关的用户帐户以及该操作的日期和时间。我们可以审核操作中的成功尝试和失败尝试。

我们可以使用这些记录尤其是失败的记录来判断系统的运行状态或者是否遭到入侵。安全审核对于任何企业系统来说都极其重要，因为只能使用审核日志来说明是否发生了违反安全的事件。如果通过其他某种方式检测到入侵，正确的审核设置所生成的审核日志将包含有关此次入侵的重要信息。

2）详述 Windows 中对账号的审计，及其对登录事件的审计等。

① 账号的审计

账号的审计用于对账号事件进行审核，包括：

* 创建、修改或删除用户帐户或组。
* 重命名、禁用或启用用户帐户。
* 设置或修改密码

根据设置系统会在任何帐户管理事件成功或者失败时生成一个审核项。在响应安全事件时，组织可以对创建、更改或删除帐户的人员进行跟踪，这一点非常重要。

② 登录事件的审计

登录事件的审计包括对计算机上登录、注销或建立网络连接的每个实例进行审核。如果正在域控制器上记录成功的帐户登录审核事件，工作站登录尝试将不生成登录审核。只有域控制器自身的交互式登录和网络登录尝试才生成登录事件。总而言之，帐户登录事件是在帐户所在的位置生成的，而登录事件是在登录尝试发生的位置生成的。

登录事件的审计对于入侵检测十分有用，攻击者的强行破解会在系统中留下大量的失败登录记录。

**心得体会**

通过本次试验我学习了Windows审计策略和安全功能的使用方法，以及事件查看器的事件查看方法、Internet选项中安全策略配置方法和windows自动升级策略的配置。本次试验使我对系统中安全策略的概念和作用有了更加深入的理解。知道了自己如何去配置自己的电脑让自己的电脑变得更加安全，受益匪浅。

**改进意见**

可以使用更新的操作系统例如win10来进行实验教学，实用意义更大。