XX大学XX学院

《网络攻击与防御》

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： | 闵新宇 |
| 组 号： | 第二组 |
| 实验日期： | 3.26 |
| 实验地点： | 寝室 |
| 实验成绩： |  |

实验报告撰写要求

实验操作是教学过程中理论联系实际的重要环节，而实验报告的撰写又是知识系统化的吸收和升华过程，因此，实验报告应该体现完整性、规范性、正确性、有效性。现将实验报告撰写的有关内容说明如下：

1、 实验报告模板为电子版。

2、 下载统一的实验报告模板，学生自行完成撰写和打印。报告的首页包含本次实验的一般信息：

*  组 号：例如：2-5 表示第二班第5组。
*  实验日期：例如：05-10-06 表示本次实验日期。(年-月-日)……
*  实验编号：例如：No.1 表示第一个实验。
*  实验时间：例如：2学时 表示本次实验所用的时间。

实验报告正文部分，从六个方面（目的、内容、步骤等）反映本次实验的要点、要求以及完成过程等情况。模板已为实验报告正文设定统一格式，学生只需在相应项内填充即可。续页不再需要包含首页中的实验一般信息。

3、 实验报告正文部分具体要求如下：

一、实验目的

本次实验所涉及并要求掌握的知识点。

二、实验环境

实验所使用的设备名称及规格，网络管理工具简介、版本等。

三、实验内容与实验要求

实验内容、原理分析及具体实验要求。

四、实验过程与分析

根据具体实验，记录、整理相应命令、运行结果等，包括截图和文字说明。

详细记录在实验过程中发生的故障和问题，并进行故障分析，说明故障排除的过程及方法。

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。

六、附录

一、实验目的

*本次实验所涉及并要求掌握的知识点。*

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

*实验所使用的设备名称及规格，网络管理工具简介、版本等。*

Windows 实验台。

三、实验内容与实验要求

*实验内容、原理分析及具体实验要求。*

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

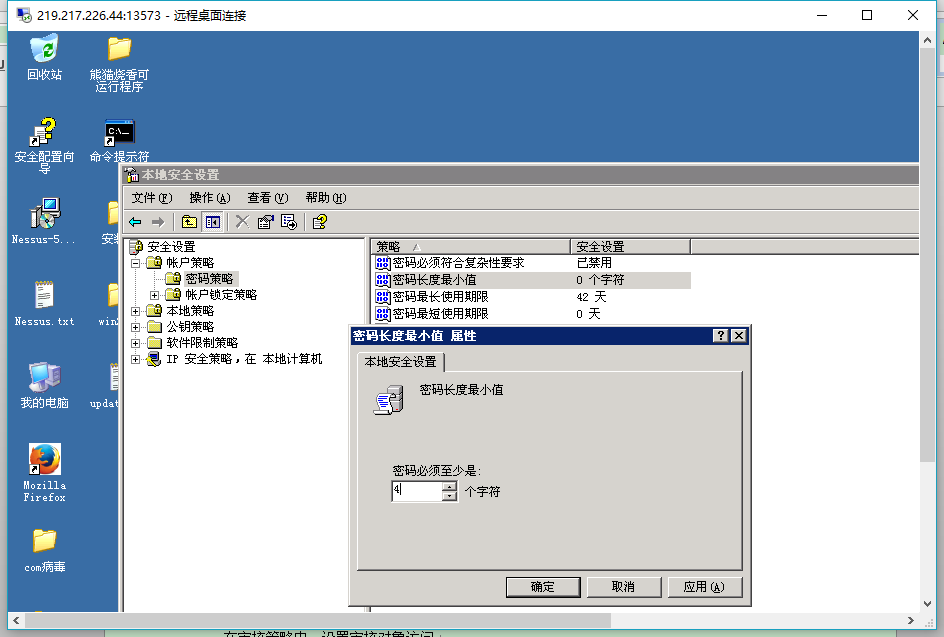
四、实验过程与分析

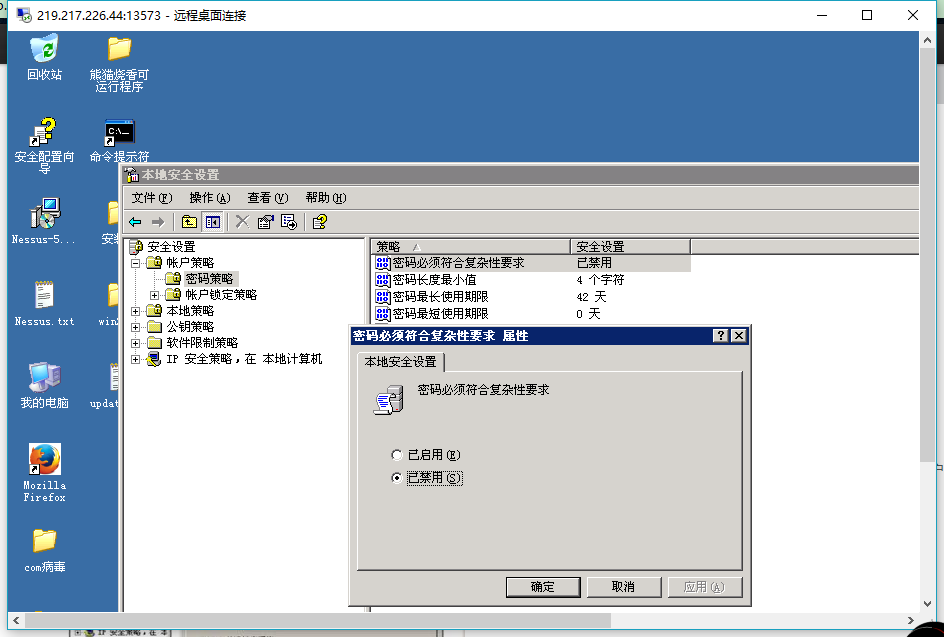
*根据具体实验，记录、整理相应命令、运行结果等，包括截图和文字说明。*

*详细记录在实验过程中发生的故障和问题，并进行故障分析，说明故障排除的过程及方法。*

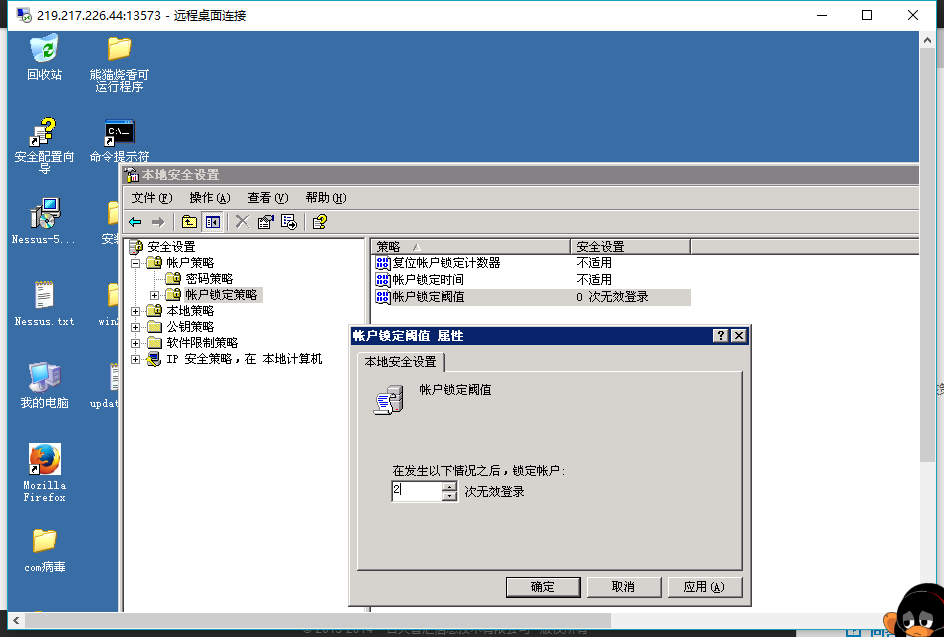
任务一：进行 Windows 操作系统的帐户策略管理

设置密码长度最小值、密码必须符合复杂性要求。



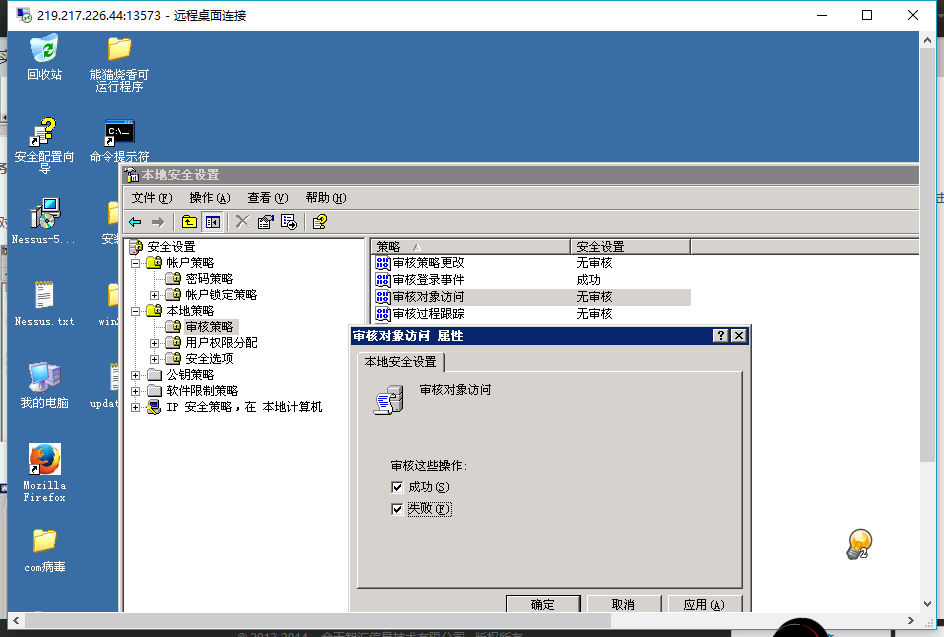


设置账户锁定阈值

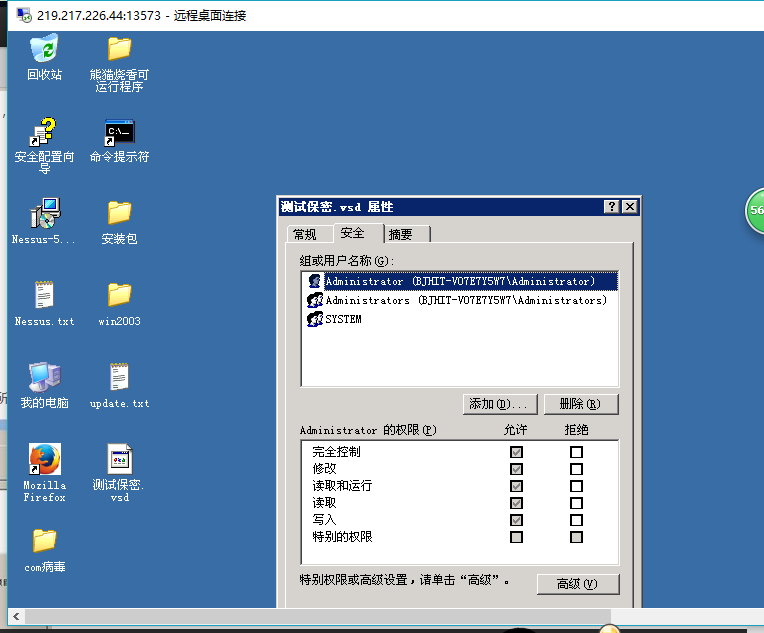


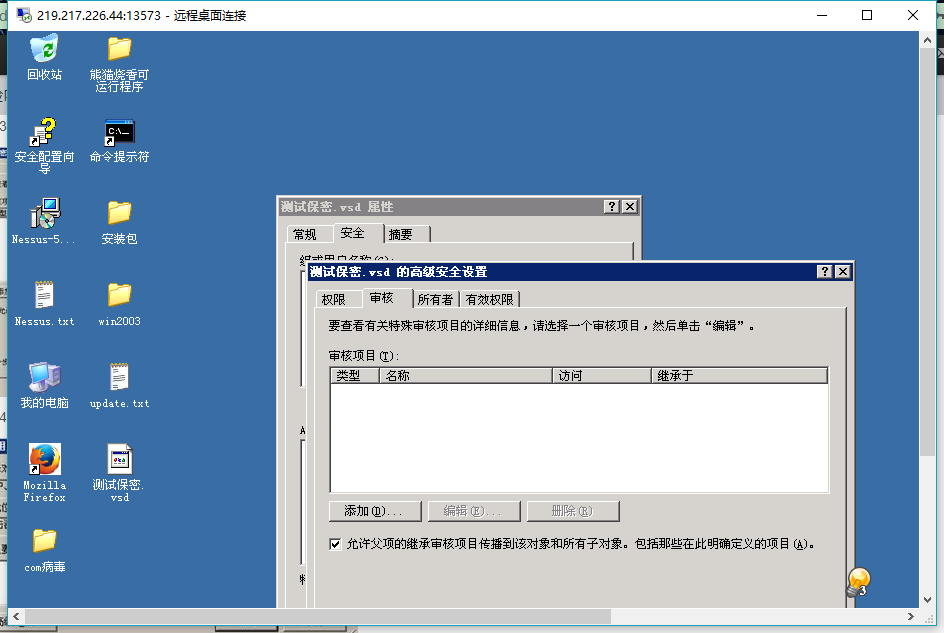
任务二：Windows 操作系统中文件操作的审计策略

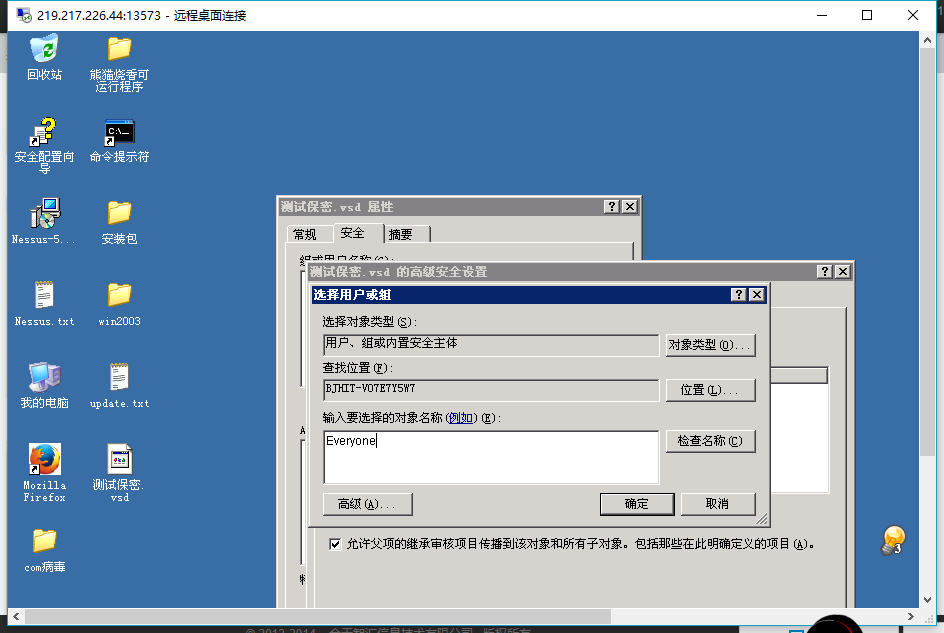
设置审核对象访问

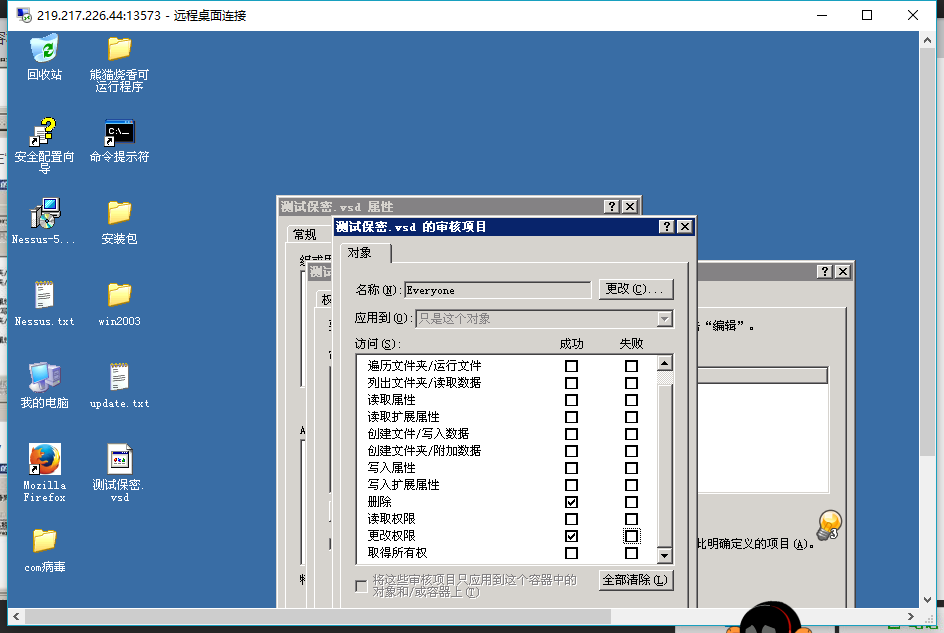


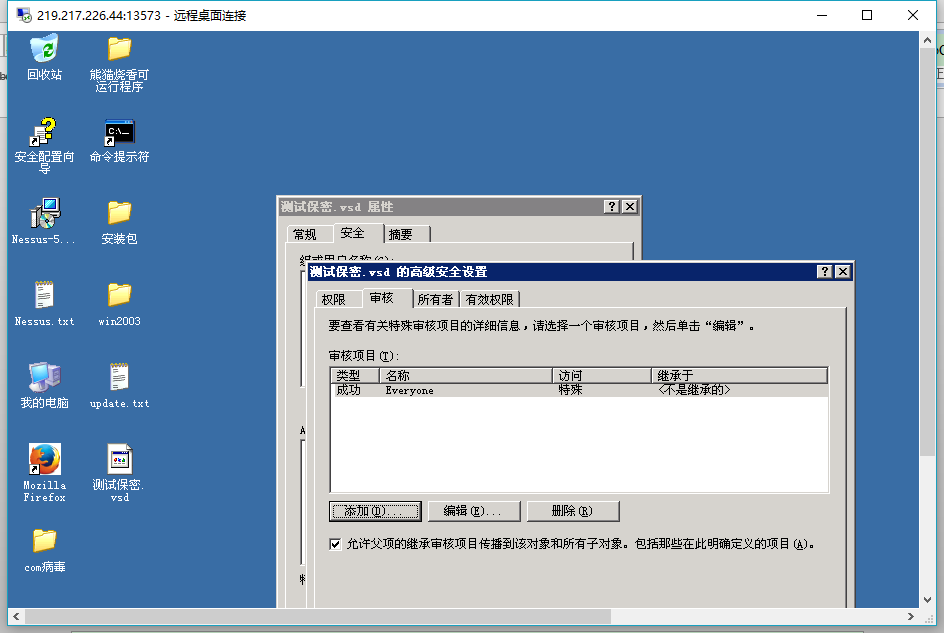
在硬盘上新建一个名为“测试保密.vsd”文件

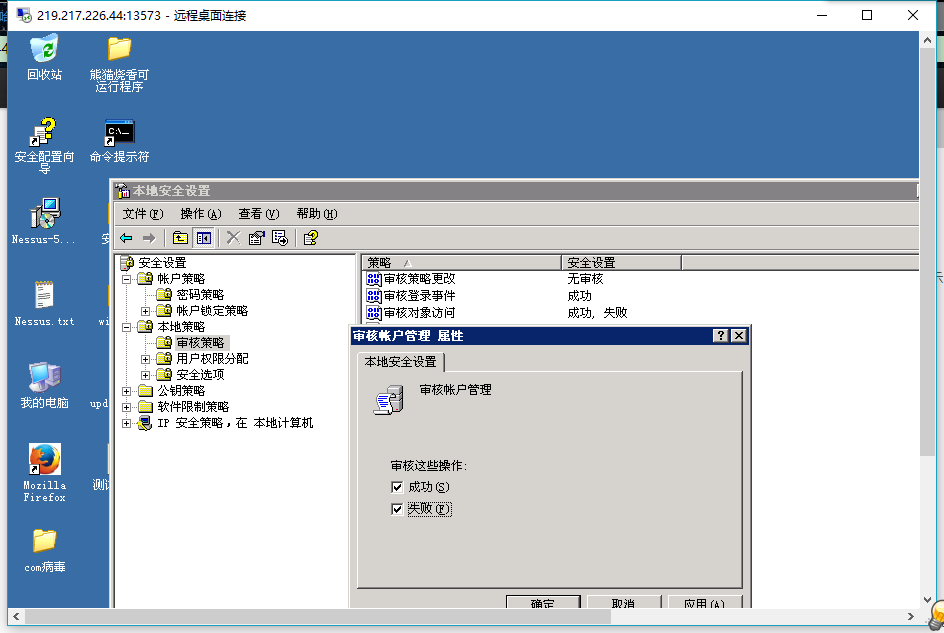




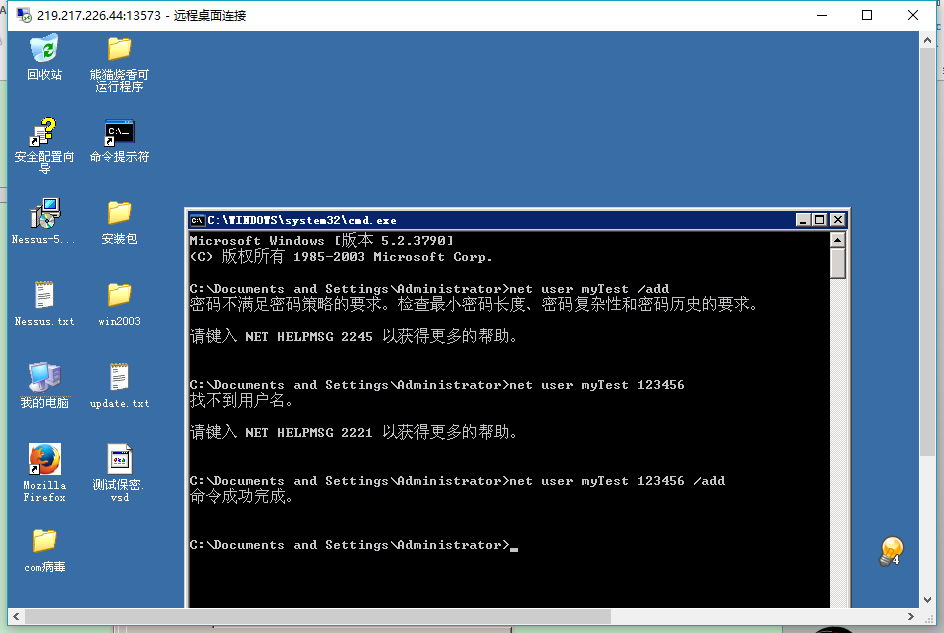


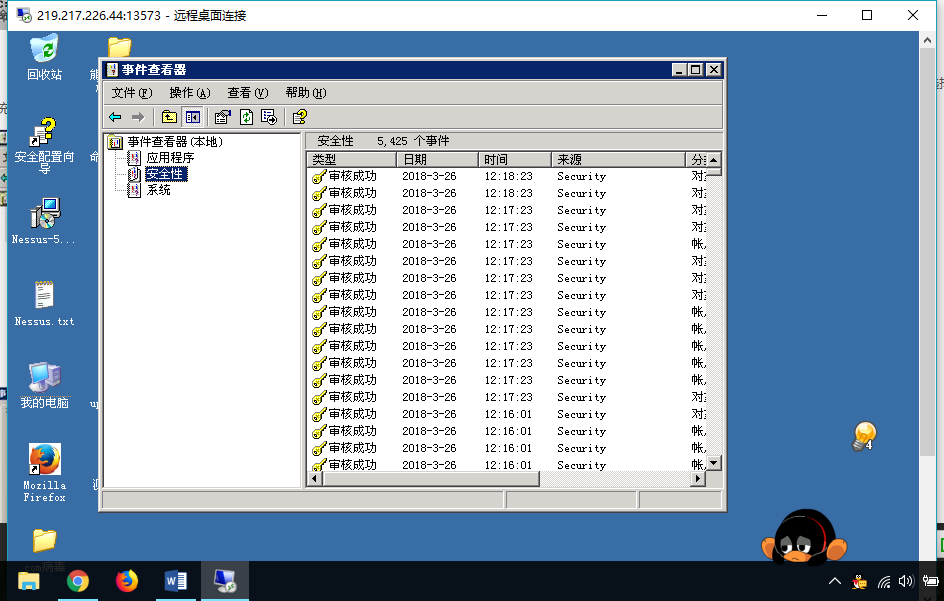


任务三：对 Windows 用户账号管理进行审计

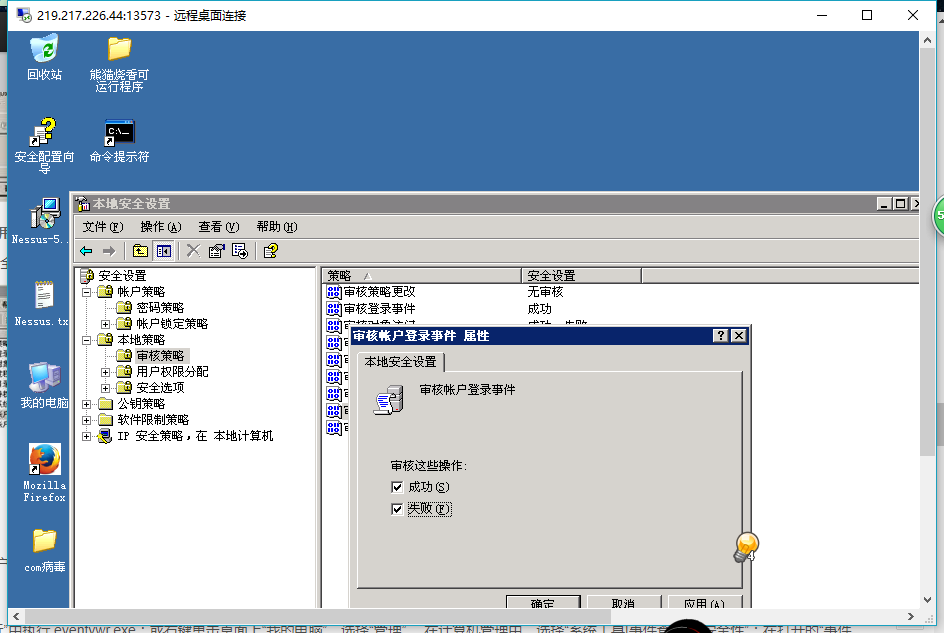


这里我把密码复杂性策略关掉了

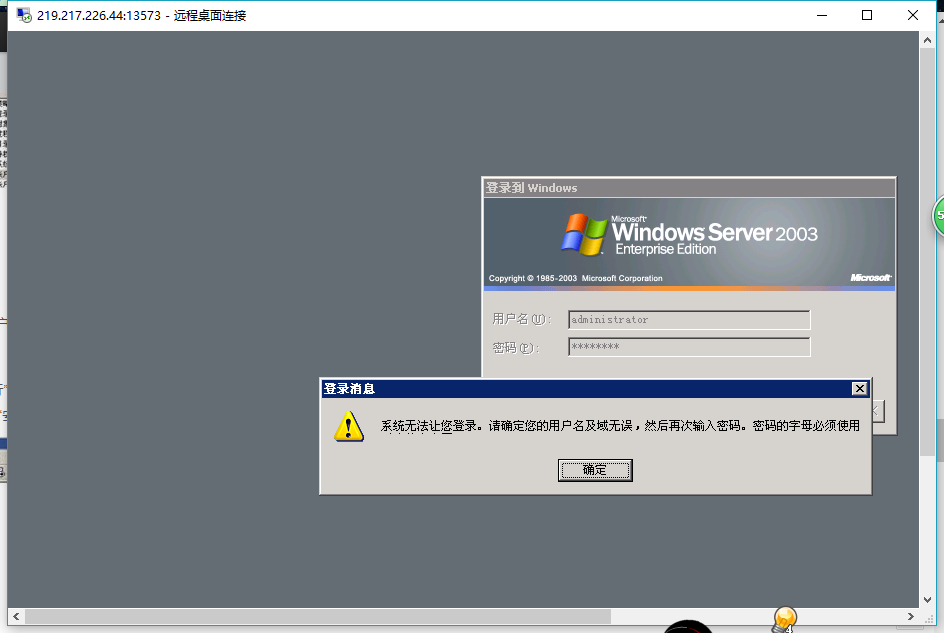


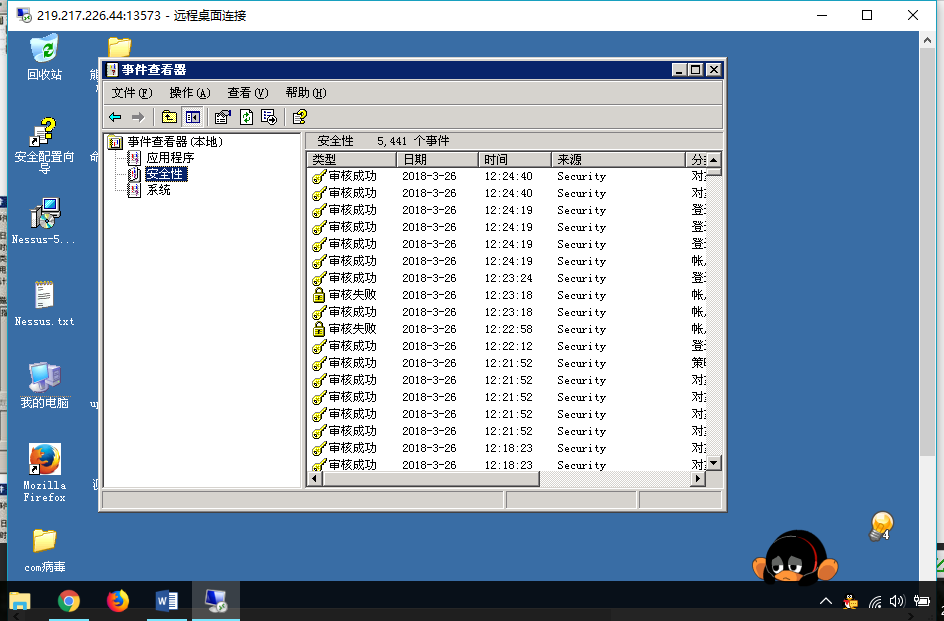


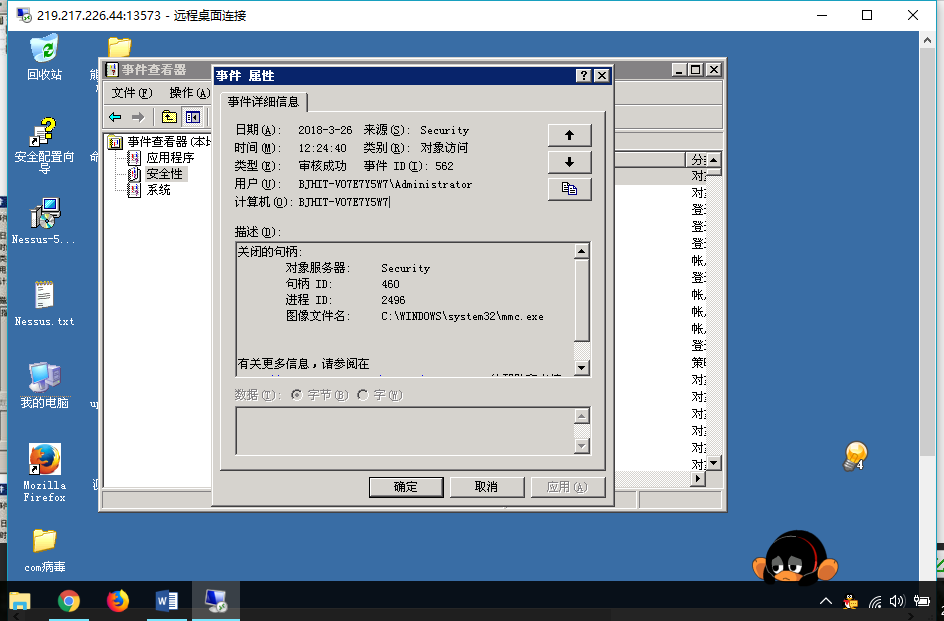
任务四：对 Windows 用户登录事件进行审计

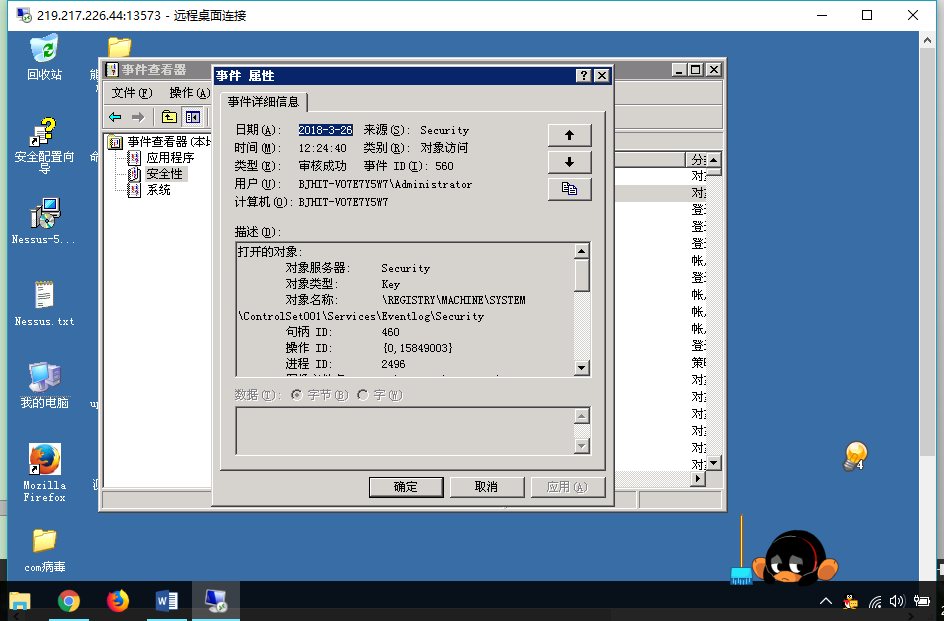


 注销当前用户，重新登录



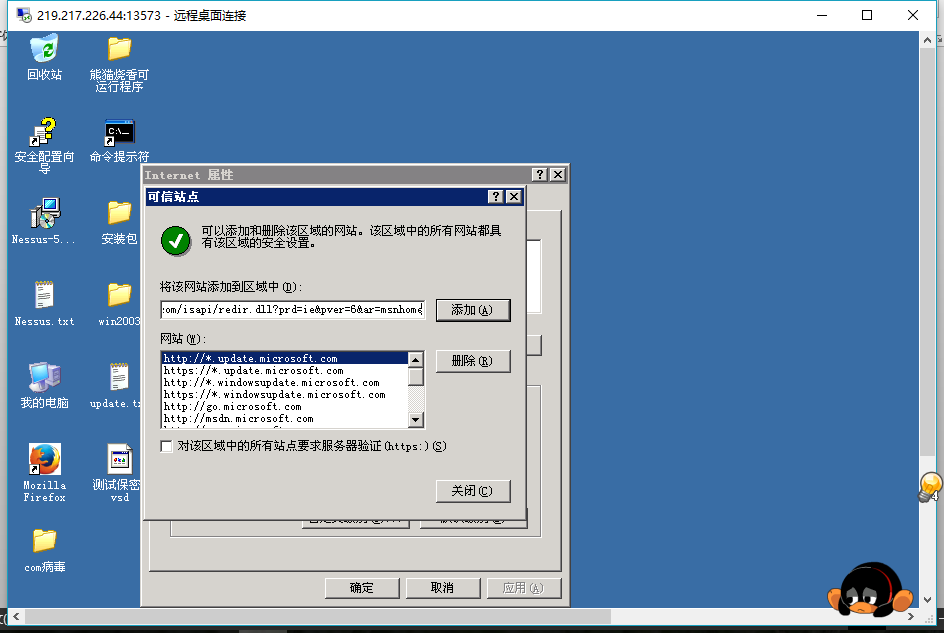


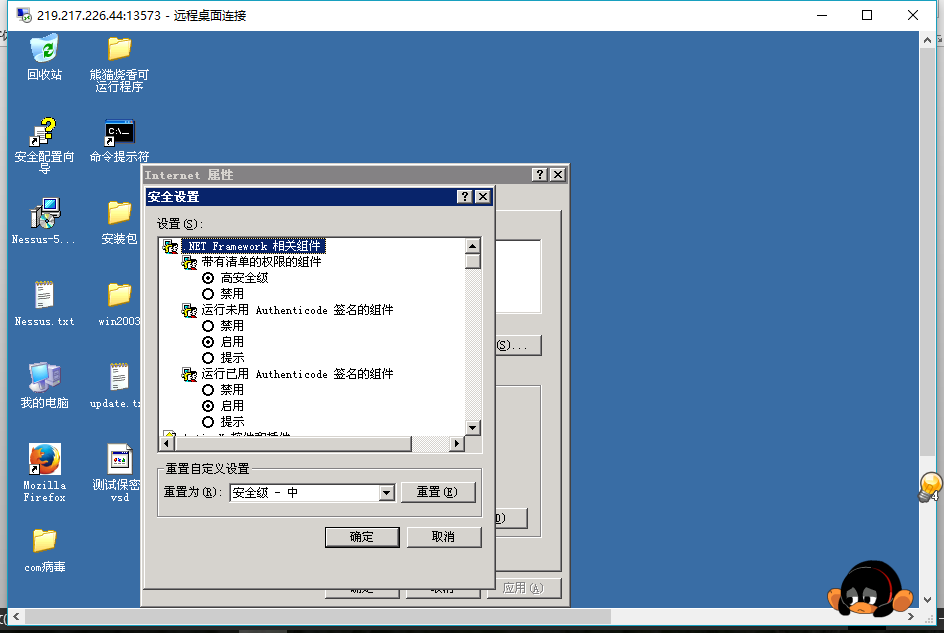




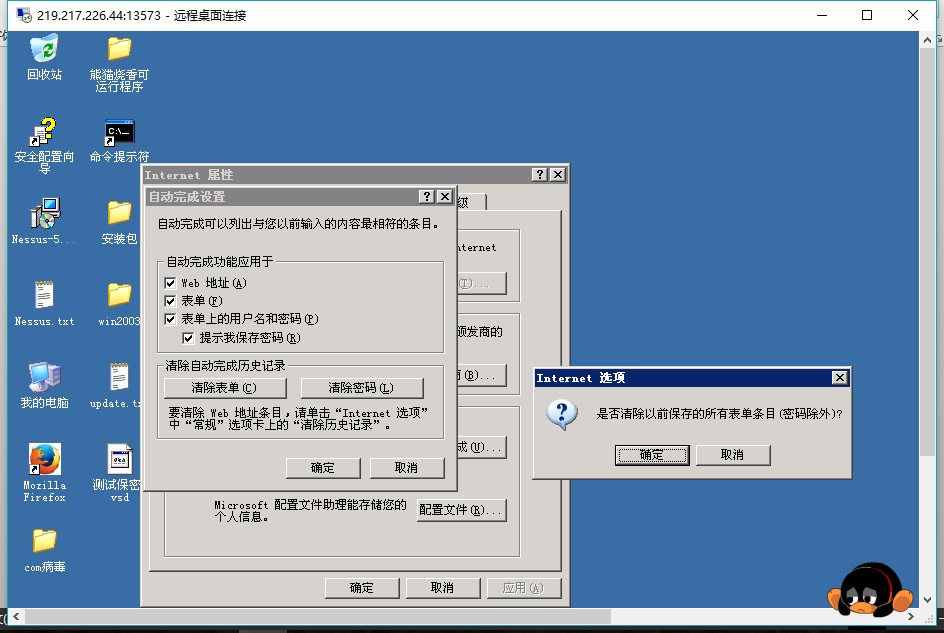
任务五：对 IE 浏览器进行安全配置

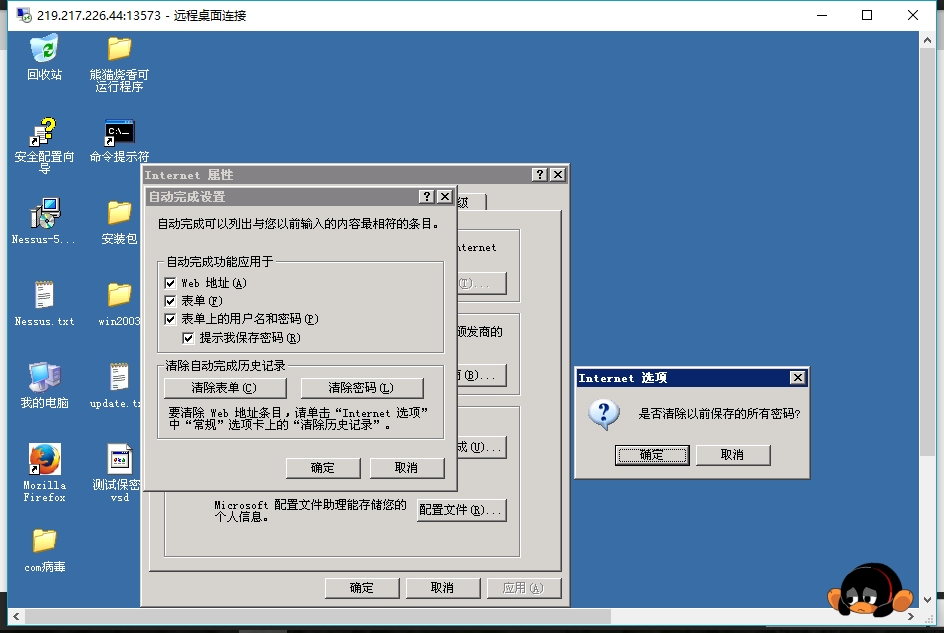












任务六：对系统补丁自动升级进行配置



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、通过本次实验，我学习到了在windows sever 2003下对本地组策略设置和审计策略的一些方法，还有查看本地事件。

2、实验中需要特别注意每一步在本地安全策略的设置，比如文件访问，账户管理，以及账户登陆。这都对后面事件查看有一定的关系。