**实验二 windows操作系统安全实验报告**

**【实验目的】**

  通过实验掌握Windows账户与密码的安全设置、文件系统的保护和加密、安全策略与安全模板的使用、审核和日志的启用、本机漏洞检测软件MBSA的使用，建立一个Windows操作系统的基本安全框架。

**【实验器材】**

   1台安装Windows2000/XP操作系统的计算机，磁盘格式配置为NTFS，预装MBSA（Microsoft Baseline Security Analyzer）工具。

**【实验内容】**

(1) Windows账户与密码的安全设置；

(2) 文件系统的保护和加密；

(3) 安全策略与安全模板的使用；

(4) 审核和日志的启用；

(5) 学会本机漏洞检测软件MBSA的使用；

  需要说明的是，下面的实验步骤主要是以 Windows2000 的设置为例进行说明，并且设置均需以管理员（ Administrator ）身份登陆系统。在 Windows 其他操作系统中，相关安全设置会稍有不同，但大同小异。

**【实验原理】**

账户和口令

  账户和口令是登录系统的基础，也是众多黑客程序攻击和窃取的对象。因此，系统账户和口令的安全是非常重要的，也是可以通过合理设置来实现的。普通常常在安装系统后长期使用系统的默认设置，忽视了Windows系统默认设置的不安全性，而这些不安全性常常被攻击者利用，通过各种手段获得合法的账户，进一步破解口令。所以，首先需要保障账户和密码安全。

文件系统

    Windows系统提供的磁盘格式有FAT，FAT32以及NTFS。其中，FAT格式和FAT32格式没有考虑对安全性方面的更高需求，例如无法设置用户访问权限等。NTFS文件系统是Windows操作系统中的一种安全的文件系统。管理员或用户可以设置每个文件夹的访问权限，从而限制一些用户和用户组的访问，以保障数据的安全。

数据加密软件EFS

   采用加密文件系统（EFS）的加密功能对敏感数据文件进行加密，可以加强数据的安全性，并且减小计算机和磁盘被窃或者被拆换后数据失窃的隐患。EFS采用了对称和非对称两种加密算法对文件进行加密，首先系统利用生成的对称密钥将文件加密成为密文，然后采用EFS证书中包含的公钥将对称密钥加密后与密文加附在一起。文件采用EFS加密后，可以控制特定的用户有权解密数据。这样即使攻击者能够访问计算机的数据存储器，也无法读取用户数据。只有拥有EFS证书的用户，采用证书中公约对应的私钥，先解密公钥加密的对称密钥，然后再用对称密钥解密密文，才能对文件进行读写操作。EFS属于NTFS文件系统的一项默认功能，同时要求使用EFS的用户必须拥有在NTFS卷中修改文件的权限。

审核与日志

    审核与日志是Windows系统中最基本的入侵监测方法。当有攻击者尝试对系统进行某些方式的攻击时，都会被安安全审核功能记录下来，写入到日志中。一些Windows下的应用程序，如IIS（Internet信息服务器），也带有相关的审核日志功能，例如，IIS的FTP日志和WWW日志等。IIS每天生成一个日志文件，包含了该日志的一切记录，例如，试图通过网络登陆系统的IP地址等，文件名通常为ex（年份）（月份）（日期），如，ex100211，就是2010年2月11日产生的日志。IIS的WWW日志在系统盘中\%systemroot%\System32\logfiles\w3svc1\目录下，FTP日志在\%Systemroot%\system32\logfiles\msftosvc1\目录下。而系统日志，安全性日志和应用程序日志分别为%Systemroot%\system32\config文件夹下的3个文件。

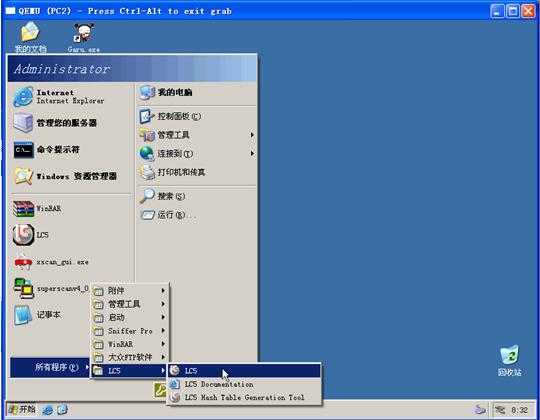
MBSA（Microsoft Baseline Security Analyzer）

    安全审计工具MBSA提供自动检查Windows系统漏洞的功能，可从微软的升级服务器中下载最新的补丁包文件，检查Windows系统中是否安装了最新的安全补丁。此外，它还可以对系统漏洞，IIS漏洞，SQLServer数据库以及IE，OFFICE等应用程序的漏洞进行扫描，以检查系统的各项配置是否符合安全性要求。

   在维护Windows操作系统安全的问题中，账号安全和文件系统安全是最基本、最容易操作的两个方面。

**【实验步骤】**

   以下设置均需以管理员（Administrator）身份登陆系统。在Windows Vista和Windows 7操作系统中，相关安全设置会稍有不同，但大同小异，下面主要以Windows XP系统的设置步骤为例进行说明。

实验步骤一：启动实验平台，拖出Windows PC机，并启动进入虚拟机环境，进入虚拟机环境。 

实验步骤二：Windows账户与密码的安全设置

 账户设置

删除不再使用的账户，禁用guest账户

共享账户，guest账户等具有较弱的安全保护，常常都是黑客们攻击的对象，系统的账户越多，被攻击者攻击成功的可能性越大，因此要及时检查和删除不必要的账户，必要时禁用guest账户。

检查和删除不必要的账户

   单击“开始”按钮，选择“管理工具”-“计算机管理”，打开的“本地用户和组”项下的 “用户”项；

    可以看到“用户”项里有添加的账户。确认各账户是否仍在使用，删除其中不用的账户。

guest账户的禁用。

为了便于观察实验结果，确保实验用机在实验前可以使用guest账户登陆；

重新打开“计算机管理”à“本地用户和组”“用户”如图所示：

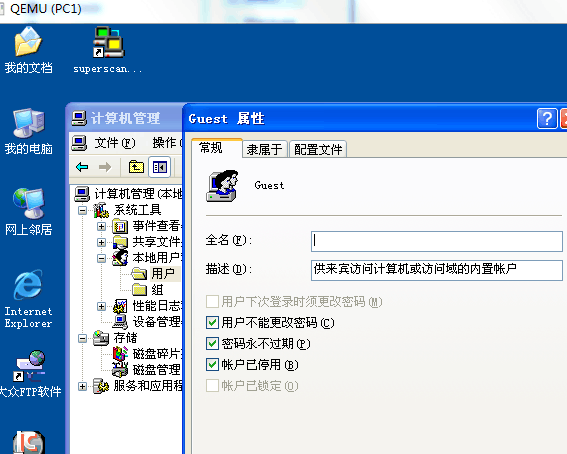


打开“管理工具”，选中“计算机管理”项，

选中其中的“本地用户和组”，打开“用户”

右键单击guest用户，弹出如图5-6所示对话框，选择“属性”，在弹出的对话框中“账户已停用”一栏前打钩。

确定后，guest钱的图标上会出现一个向下方向箭头的标识。此时再次试用guest账户登陆，则会显示“您的账户已被停用，请与管理员联系”。



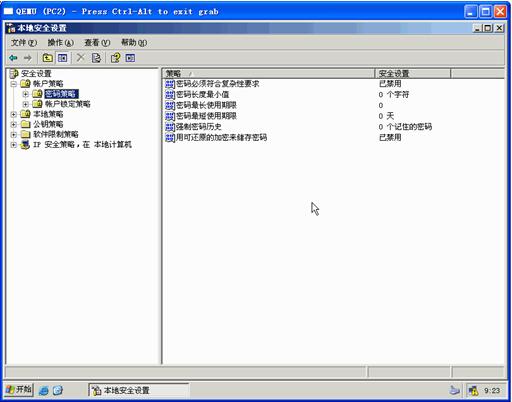
启用账户策略

账户策略设置：

账户策略是Windows账户管理的重要工具。

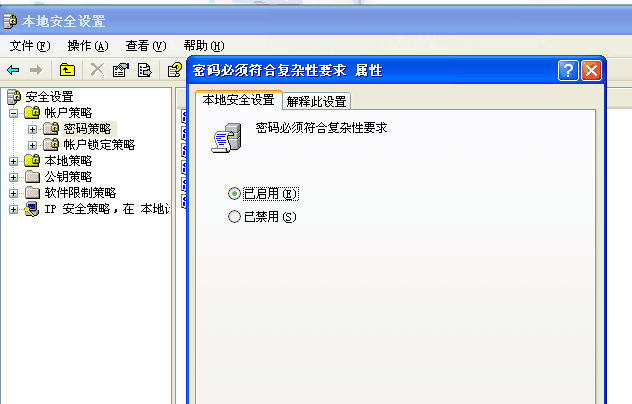
打开“开始”->“管理工具”->“本地安全策略”，选择“账户策略”

双击“密码策略”，密码策略用于决定系统密码的安全规则和设置。

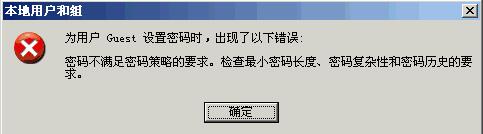


其中，符合复杂性要求的密码是具有相当长度，同时含有数字、大小写字母和特殊字符的序列。双击其中每一项，可按照需要改变密码特性的设置。

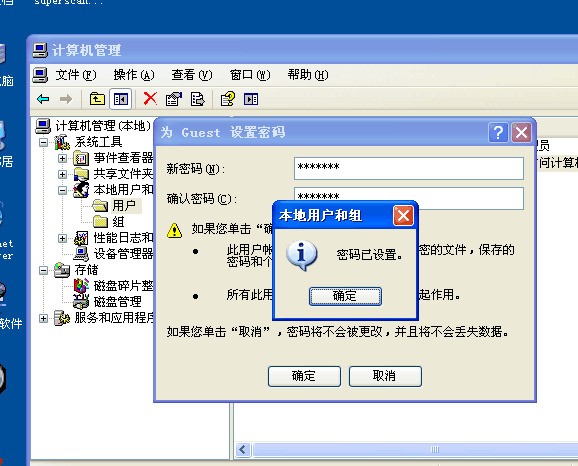
（1）.双击“密码必须符合复杂性要求”，选择“启用”；



下面我们看一下策略是否启动，打开“计算机管理”—>“本地用户和组”中的“用户”项，对话框中选择一个用户后，右键单击账户，选择“更改密码”。弹出“更改密码”的窗口后，此时设置的密码要符合设置的密码要求。例如，若输入密码为123，则弹出如图所示的对话框：



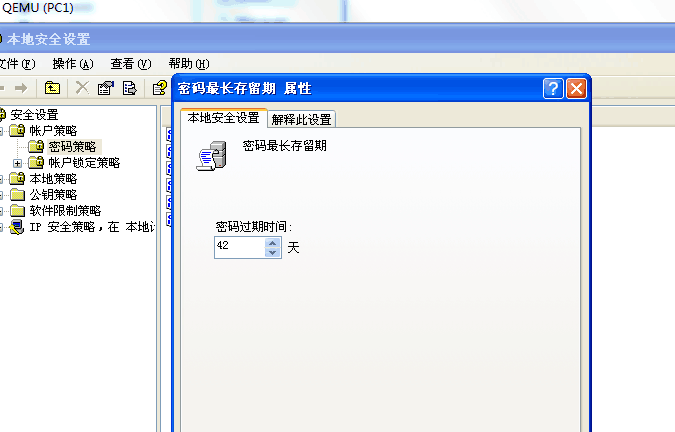
若输入密码为yc++123，密码被系统接收。



(2)双击面板中“密码长度最小值”，在弹出的的对话框中设置可被系统接纳的账户密码长度最小值，例如设置为6个字符。一般为了达到较高的安全性，建议密码长度的最小值为8。



（3）双击面板中“密码最长存留期”，在弹出的对话框中设置系统要求的账户密码的最长使用期限为42天。设置密码自动保留期，可以提醒用户定期修改密码，防止密码使用时间过长带来的安全问题。



（4）双击面板中“密码最短存留期”，在弹出的对话框中修改设置密码最短存留期为7天。在密码最短存留期内用户不能修改密码。这项设置时为了避免入侵的攻击者修改账户密码。

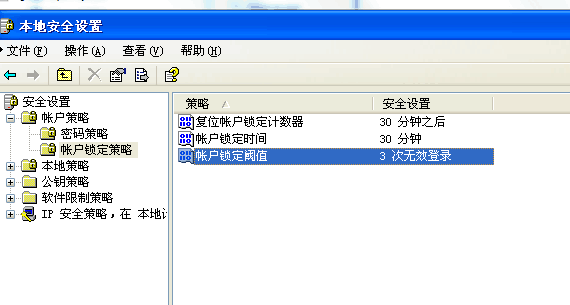
（5）双击“强制密码历史”和“为域中所有用户使用可还原的加密储存密码”，在相继弹出的类似对话框中，设置让系统记住的密码数量和是否设置加密存储密码。

    至此，密码策略设置完毕。

账户锁定策略设置：

    在账户策略中的第二项是账户锁定策略，它决定系统锁定账户的时间等相关设置。

    打开 “账户锁定策略”，弹出如图所示的窗口。



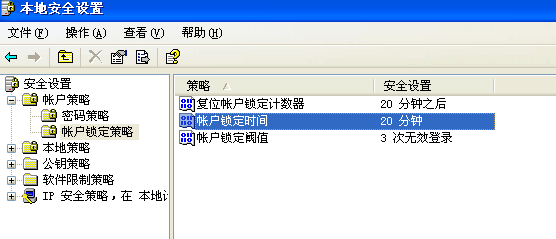
双击“账户锁定阈值”，

在弹出的对话框中设置账户被锁定之前经过的无效登陆次数（如3次），以便防范攻击者利用管理员身份登陆后无限次的猜测账户的密码（穷举法攻击）。



双击“账户锁定时间”

在弹出的对话框中设置账户被锁定的时间（如20min）。此后，当某账户无效登陆（如密码错误）的次数超过3次时，系统将锁定该账户20min。

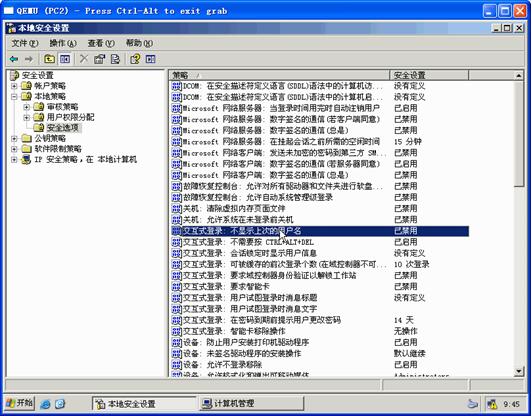


开机时设置为“不自动显示上次登陆账户”

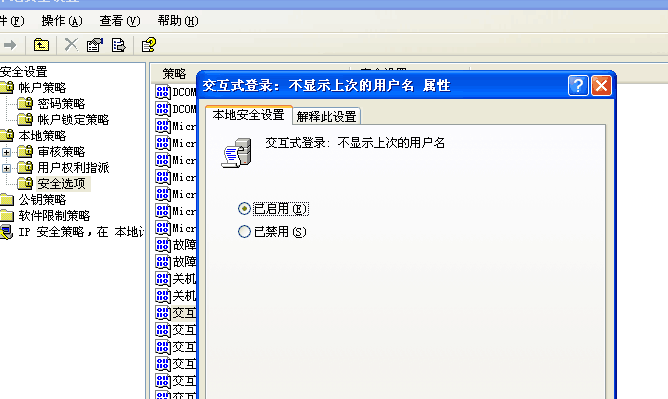
Windows默认设置为开机时自动显示上次登陆的账户名，许多用户也采用了这一设置。这对系统来说是很不安全的，攻击者会从本地或Terminal Service的登录界面看到用户名。

要禁止显示上次的登录用户名，可做如下设置：

单击“开始”按钮，打开“开始”中“管理工具”下的“本地安全策略”，选择“本地策略”下的“安全选项”，如图所示：

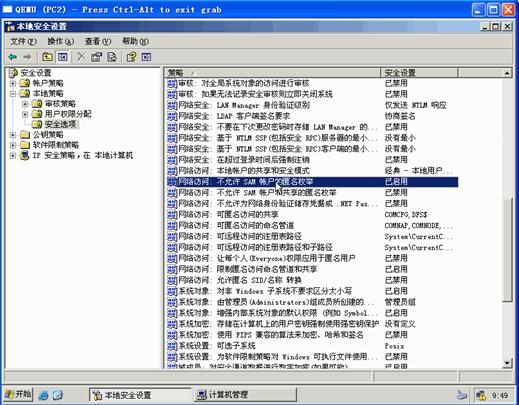


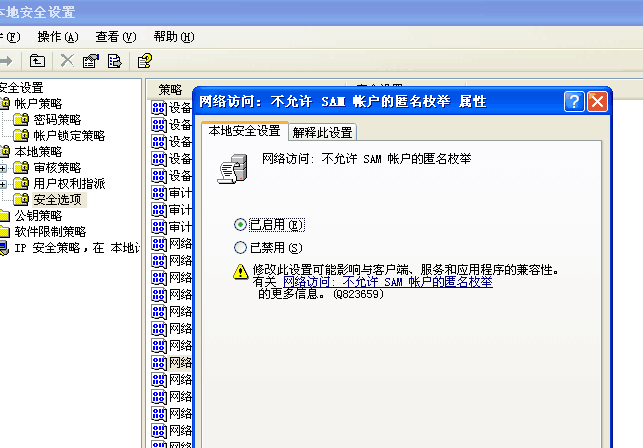
并在所示窗口右侧列表中选择“交互式登录”双击，弹出如图5-20所示对话框，选择“已启用”，完成设置。



禁止枚举账户名

打开“管理工具”选项，双击“本地安全策略”项，选择“本地策略”中的“安全选项”， 并在弹出的窗口右侧列表中选择“对匿名连接的额外限制”项，在“本地策略设置”中选择“不允许枚举 SAM 账户和共享”，如图。





此外，在“安全选项”中还有多项增强系统安全的选项，请同学们自行查看。

实验步骤三：文件系统的保护和加密

打开采用NTFS格式的磁盘，选择一个需要设置用户权限的文件夹。这里选择C盘下的“tools”文件夹（此文件夹根据个人需要，可对不同文件夹进行操作）。

右键单击该文件夹，选择“属性”，在工具栏中选择“安全”，弹出如图所示的窗口。



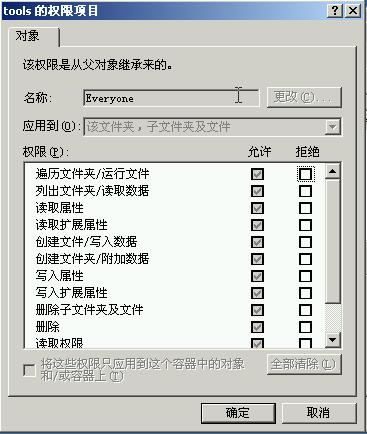
单击“高级”，在弹出的如图所示的窗口中选择“权限”，打开后在弹出的窗口中将“允许将来自父系的可继承权限传播给该对象”之前的勾去掉，以去掉来自父系文件夹的继承权限（如不去掉则无法删除可对父系文件夹操作用户组的操作权限）。



选中列表中的 Everyone 组，单击“删除”按钮，删除 Everyone 组的操作权限，由于新建的用户往往都归属于 Everyone 组，而 Everyone 组在缺省情况下对所有系统驱动器都有完全控制权，删除 Everyone 组的操作权限可以对新建用户的权限进行限制，原则上只保留允许访问此文件夹的用户和用户组。

选择相应的用户组，在对应的复选框中打勾，设置其余用户组对该文件夹的操作权限。

单击“高级”按钮，在弹出的窗口中，查看各用户组的权限，如下图所示查看Everyone组权限：



注销计算机，用不同的用户登陆，查看 C 盘“tools”文件夹的访问权限，将结果记录在实验报告中。

步骤四 启用安全策略与安全模块

启用安全模板

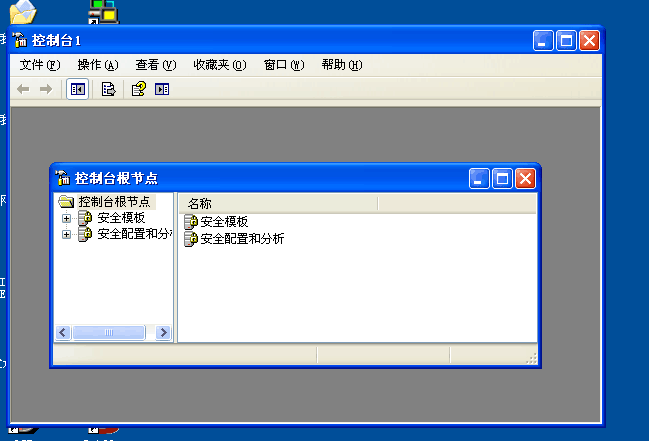
开始前，请记录当前系统的账户策略和审核日志状态，便于同实验后的设置进行比较。

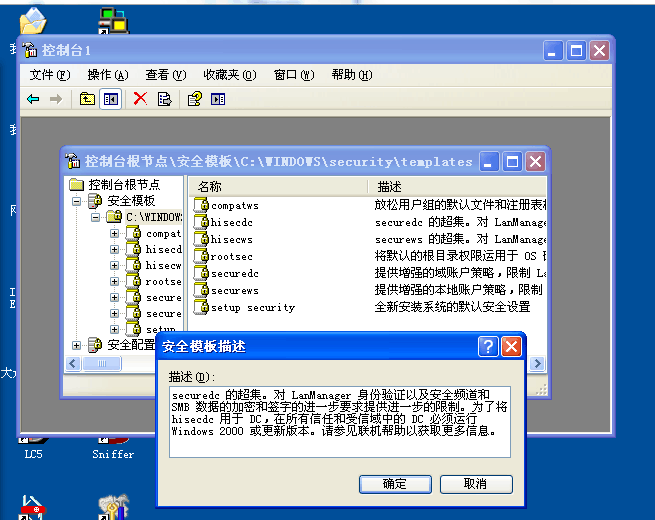
⑴ 单击“开始”按钮，选择“运行”按钮，在对话框中运行 mmc ，打开系统控制台，如下图所示：



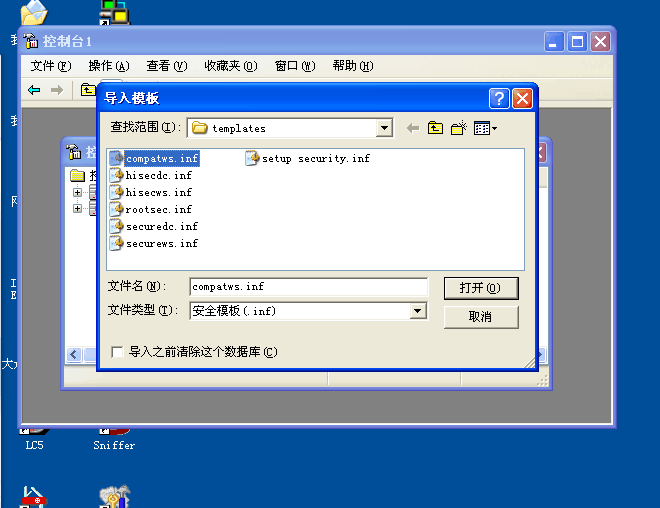
⑵ 单击工具栏上“控制台”，在弹出的菜单中选择“添加 / 删除管理单元”，单击“添加”，在弹出的窗口中分别选择“安全模板”、“安全设置和分析”，如图单击“添加”按钮后，关闭窗口，并单击“确定”按钮。

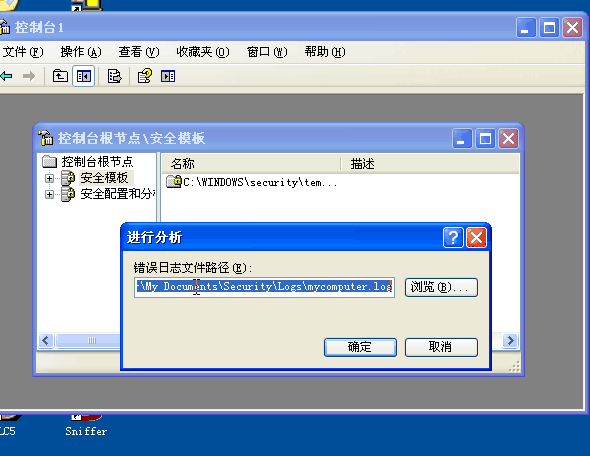
⑶ 此时系统控制台中根节点下添加了“安全模板”、“安全设置分析”两个文件夹，打开“安全模板”文件夹，可以看到系统中存在的安全模板。右键单击模板名称，选择“设置描述”，可以看到该模板的相关信息。选择“打开”，右侧窗口出现该模板的安全策略，如图所示，双击每中安全策略可看到其相关配置。





⑷ 右键单击“安全设置与分析”，选择“打开数据库”。在弹出的对话框中输入预建安全数据库的名称，例如起名为 mycomputer.sdb ，单击“打开”按钮，在弹出的窗口中，根据计算机准备配置成的安全级别，选择一个安全模板将其导入。

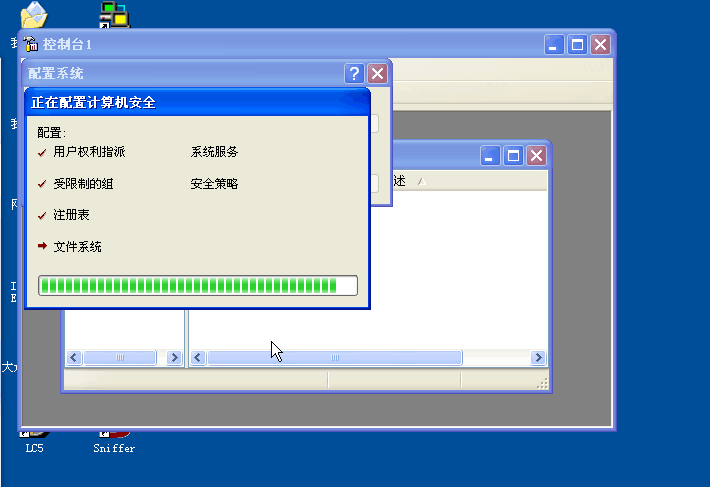




⑸ 右键单击“安全设置与分析”，选择“立即分析计算机”，单击“确定”按钮，系统开始按照上一步中选定的安全模板，对当前系统的安全设置是否符合要求进行分析。将分析结果记录在实验报告中。



⑹ 右键单击“安全设置与分析”，选择“立即配置计算机”，则按照第（ 4 ）步中所选的安全模板的要求对当前系统进行配置。



⑺ 在实验报告中记录实验前系统的缺省配置，接着记录启用安全模板后系统的安全设置，记录下比较和分析的结果。

2 ．建安全模板

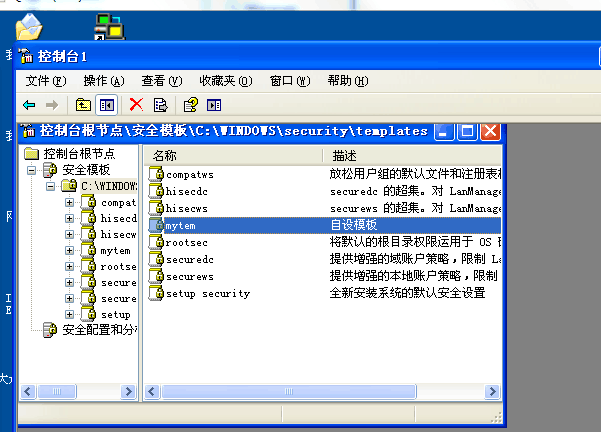
⑴ 单击“开始”按钮，选择“运行”按钮，在对话框中运行 mmc ，打开系统控制台。

⑵ 单击工具栏上“控制台”，在弹出的菜单中选择“添加 / 删除管理单元”，单击“添加”，在弹出的窗口中分别选择“安全模板”、“安全设置和分析”，单击“添加”按钮后，关闭窗口，并单击“确定”按钮。

⑶ 此时系统控制台中根节点下添加了“安全模板”、“安全设置分析”两个文件夹，打开“安全模板”文件夹，可以看到系统中存在的安全模板。右键单击模板名称，选择“设置描述”，可以看到该模板的相关信息。选择“打开”，右侧窗口出现该模板的安全策略，双击每中安全策略可看到其相关配置。

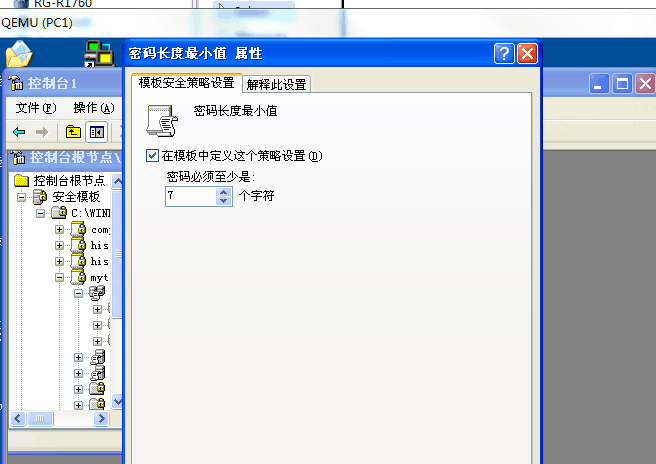
⑷ 右键单击“安全设置与分析”，选择“打开数据库”。在弹出的对话框中输入预建安全数据库的名称，例如起名为 mycomputer.sdb ，单击“打开”按钮，在弹出的窗口中，根据计算机准备配置成的安全级别，选择一个安全模板将其导入。

⑸ 展开“安全模板”，右键单击模板所在路经 , 选择“新加模板”，在弹出的对话框中添如预加入的模板名称 mytem ，在“安全模板描述“中填入“自设模板”。查看新加模板是否出现在模板列表中。

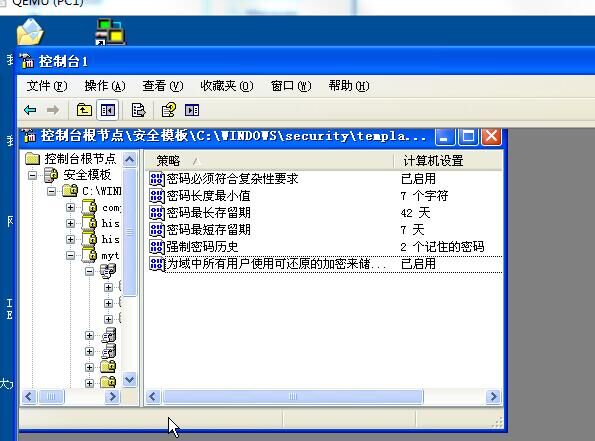


⑹ 双击 mytem ，在现实的安全策略列表中双击“账户策略”下的“密码策略”，可发现其中任一项均显示“没有定义”，双击预设置的安全策略（如“密码长度最小值”）.

⑺ 在“在模板中定义这个策略设置”前打勾，在框中填如密码的最小长度为 7 。



⑻ 依次设定“账户策略”、“本地策略”等项目中的每项安全策略，直至完成安全模板的设置。



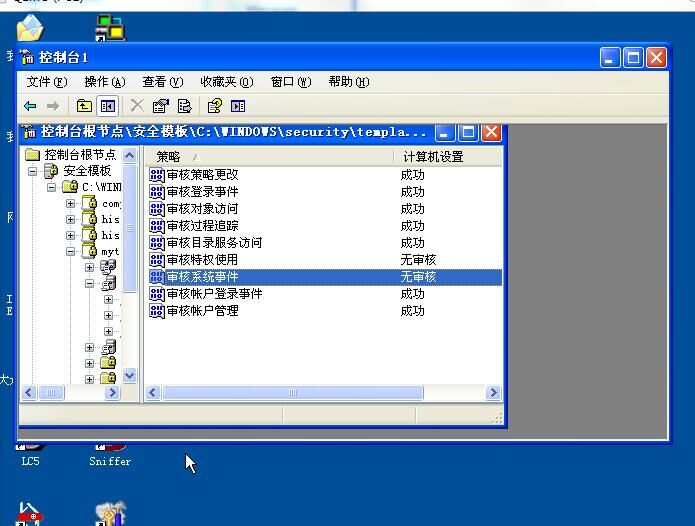
**步骤五  启用审核与日志查看**

打开审核策略

打开“开始”中的“管理工具”，选择“本地安全策略；

打开“本地策略”中的“审核策略”，可以看到当前系统的审核策略。

双击每项策略可选择是否启用该项策略。例如“审核账户管理”将对每次建立新用户、删除用户等操作进行记录，“审核登陆事件”将对每次用户的登录进行记录；“审核过程追踪”将对每次启动或者退出的程序或者进程进行记录，根据需要启用相关审核策略。审核策略启用后，审核结果放在各自事件日志中。



查看事件日志

打开“开始”中的“管理工具”，双击“事件查看器”，如图5-38所示，可以看到Win 7的3种日志，其中安全日志用于记录刚才上面审核策略中所设置的安全事件。双击Windows日志下的“安全日志”，可查看有效无效、登录尝试等安全事件的具体记录。

