实验 3　Windows 操作系统的安全设置

视频讲解

3.1　实验目的及要求

3.1.1　实验目的

通过实验掌握 Windows 操作系统的常用基本安全设置、有效防范攻击的措施、Windows 账户和密码的安全设置、文件系统的保护和加密、安全策略和安全模板的使用、审核和日志的启用、数据的备份与还原，建立一个 Windows 操作系统的基本安全框架。

3.1.2　实验要求

根据教材中介绍的 Windows 操作系统的各项安全性实验要求，详细观察并记录设置前后系统的变化，给出分析报告。

3.1.3　实验设备及软件

一台安装 Windows XP 操作系统的计算机，磁盘格式配置为 NTFS。

3.2　禁止默认共享

1. 什么是默认共享

Windows 2000/XP/2003 版本的操作系统提供了默认共享功能，这些默认的共享都有 $ 标志，意为“隐含的”，包括所有的逻辑盘(C$，D$，E$ 等)和系统目录(admin$)。

2. 带来的问题

微软公司的初衷是便于网管进行远程管理，这虽然方便了局域网用户，但对个人用户来说这样的设置是不安全的。如果计算机联网，网络上的任何人都可以通过共享硬盘随意进入别人的计算机，所以有必要关闭这些共享。Windows XP 在默认安装后允许任何用户通过空用户连接(IPC$)得到系统所有账户和共享列表，任何远程用户都可以利用这个空的连接得到目标主机上的用户列表。黑客就利用这项功能查找系统的用户列表，并使用一些字典工具对系统进行攻击。这就是网上较流行的 IPC 攻击。

3. 查看本地共享资源

执行“开始”→“运行”命令，在打开的对话框中输入 cmd，在命令行窗口中输入 net share，如图 3.1 所示，如果看到有异常的共享，那么应该关闭。但是有时关闭共享后，在下次开机的时候又出现了，那么就应该考虑一下，计算机是否已经被黑客控制了，或者中了病毒。

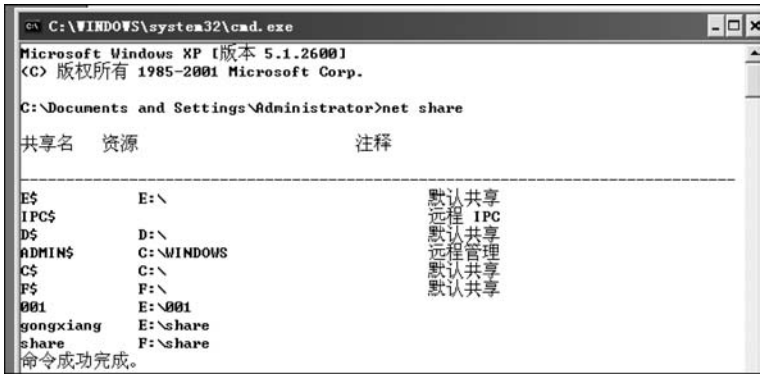


图 3.1 本地共享资源

4. 删除共享(每次输入一个)

```
net share admin$ /delete
net share c$ /delete
net share d$ /delete
net share e$ /delete
net share f$ /delete
```

注意:如果有 g 和 h,可以继续删除。

5. 注册表改键值法——关闭默认共享漏洞

运行“开始”→“运行”命令,在打开的对话框中输入 regedit,单击“确定”按钮,打开注册表编辑器,找到 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\lanmanserver\parameters 项,双击右侧窗口中的 AutoShareServer 项将键值设为 0,这样就能关闭硬盘各分区的共享。如果没有 AutoShareServer 项,可自己新建一个类型为 REG_DWORD、键值为 0 的 DWORD 值。然后,还是在这一窗口中找到 AutoShareWks 项,类型为 REG_DWORD,也将键值设为 0,关闭 admin$ 共享,如图 3.2 所示。

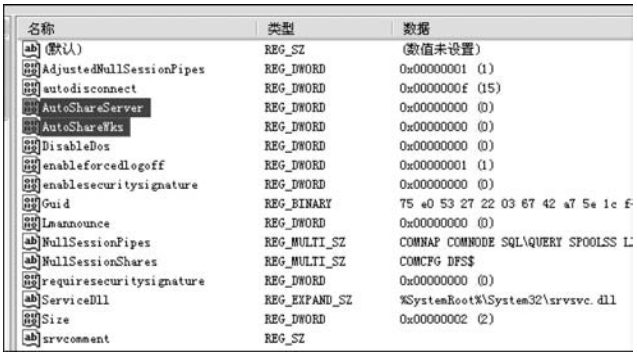
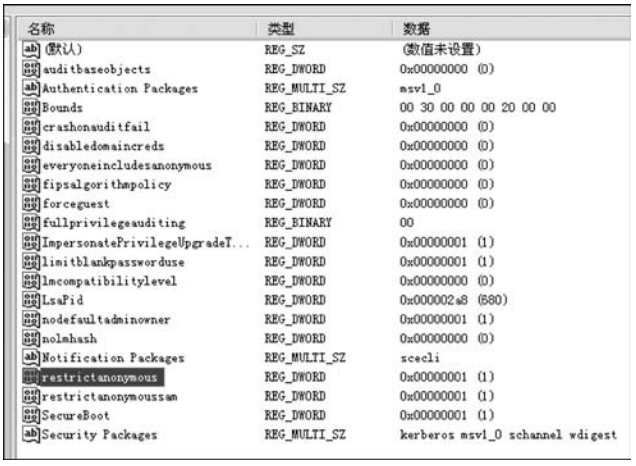


图 3.2 修改键值(1)

最后到 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa 处找到 restrictanonymous 项,将键值设为 1。如果设置为 1,一个匿名用户仍然可以连接到 IPC$ 共享,但限制通过这种连接得到列举 SAM(Security Account Manager)账号和共享等信息。在 Windows 2000 中增加了键值 2,限制所有匿名访问,除非特别授权。如果设置为

2 的话,可能会有一些其他问题发生,建议设置为 1。如果上面所说的主键不存在,就新建一个修改键值,如图 3.3 所示。



名称	类型	数据
(默认)	REG_SZ	(数值未设置)
auditbaseobjects	REG_DWORD	0x00000000 (0)
Authentication Packages	REG_MULTI_SZ	msv1_0
Bounds	REG_BINARY	00 30 00 00 00 20 00 00
crashonauditfail	REG_DWORD	0x00000000 (0)
disabledomaincreds	REG_DWORD	0x00000000 (0)
everyoneincludesanonymous	REG_DWORD	0x00000000 (0)
fipsalgorithmpolicy	REG_DWORD	0x00000000 (0)
forceguest	REG_DWORD	0x00000000 (0)
fullprivilegeauditing	REG_BINARY	00
ImpersonatePrivilegeUpgradeT...	REG_DWORD	0x00000001 (1)
limitblankpassworduse	REG_DWORD	0x00000001 (1)
lmcompatibilitylevel	REG_DWORD	0x00000000 (0)
LsaPid	REG_DWORD	0x000002a8 (680)
nodefaultadminowner	REG_DWORD	0x00000001 (1)
nolmhash	REG_DWORD	0x00000000 (0)
Notification Packages	REG_MULTI_SZ	scecli
restrictanonymous	REG_DWORD	0x00000001 (1)
restrictanonymoussam	REG_DWORD	0x00000001 (1)
SecureBoot	REG_DWORD	0x00000001 (1)
Security Packages	REG_MULTI_SZ	kerberos msv1_0 schannel wdigest

图 3.3　修改键值(2)

注意:修改注册表后必须重启计算器才能生效,但一经改动就会永远停止共享。

3.3　服 务 策 略

若个人计算机没有特殊用途,基于安全考虑,打开“控制面板”,选择“管理工具”→“服务”,如图 3.4 所示。

服务(本地)

Alerter

启动此服务

描述:
通知所选用户和计算机有关系统管理级警报。如果服务停止,使用管理警报的程序将不会受到它们。如果此服务被禁用,任何直接依赖它的服务都将不能启动。

名称	描述	状态	启动类型
Alerter	通知所选用户和计算机有关系统管理级...		手动
Application Layer Gateway Service	为 Internet 连接共享和 Windows 防...	已启动	手动
Application Management	提供软件安装服务,诸如分派,发行以...		手动
Background Intelligent Transfer Service	在后台传输客户端和服务器之间的数据...		手动
ClipBook	启用“剪贴簿查看器”储存信息并与远...		已禁用
COM+ Event System	支持系统事件通知服务(SENS),此服务...	已启动	手动
COM+ System Application	管理 基于COM+ 组件的配置和跟踪。如...		手动
Computer Browser	维护网络上计算机的更新列表,并将列...	已启动	自动
Cryptographic Services	提供三种管理服务:编录数据库服务,...	已启动	自动
DCOM Server Process Launcher	为 DCOM 服务提供加载功能。	已启动	自动
DHCP Client	通过注册和更改 IP 地址以及 DNS 名...	已启动	自动
Distributed Link Tracking Client	在计算机内 NTFS 文件之间保持链接或...	已启动	自动
Distributed Transaction Coordinator	协调跨多个数据库、消息队列、文件系...		手动
DNS Client	为此计算机解析和缓冲域名系统 (DNS)...	已启动	自动
Event Log	启用在事件查看器查看基于 Windows ...	已启动	自动
Extensible Authentication Protocol Ser...	向 Windows 客户端提供可扩展身份验...		手动
Fast User Switching Compatibility	为在多用户下需要协助的应用程序提供...	已启动	手动
Health Key and Certificate Management ...	管理健康证书和密钥(由 NAP 使用)		手动
Help and Support	启用在此计算机上运行帮助和支持中心...		手动
HTTP SSL	此服务通过安全套接字层(SSL)实现 HT...		手动
Human Interface Device Access	启用对智能界面设备 (HID)的通用输入...		已禁用
IMAPI CD-Burning COM Service	用 Image Mastering Applications Fr...		手动
Indexing Service	本地和远程计算机上文件的索引内容和...		手动
IPSEC Services	管理 IP 安全策略以及启动 ISAKMP/Oa...	已启动	自动
Logical Disk Manager	监测和监视新硬盘驱动器并向逻辑磁盘...	已启动	自动
Logical Disk Manager Administrative Se...	配置硬盘驱动器和卷。此服务只为配置...		手动
Messenger	传输客户端和服务器之间的 NET SEND ...	已启动	手动
MS Software Shadow Copy Provider	管理卷影复制服务拍摄的软件卷影复制...		手动
Net Logon	支持网络上计算机 pass-through 帐户...		手动
NetMeeting Remote Desktop Sharing	使授权用户能够通过使用 NetMeeting ...		手动
Network Access Protection Agent	允许 Windows 客户端参与网络访问保护		手动
Network Connections	管理“网络和拨号连接”文件夹中对象...	已启动	手动
Network DDE	为在同一台计算机或不同计算机上运行...		已禁用
Network DDE DSDM	管理动态数据交换 (DDE) 网络共享。...		已禁用

图 3.4　服务选项

禁用以下服务。

- Alerter：通知所选用户和计算机有关系统管理级警报。
- ClipBook：启用“剪贴簿查看器”储存信息并与远程计算机共享。
- Human Interface Device Access：启用对智能界面设备(HID)的通用输入访问，它激活并保存键盘、远程控制和其他多媒体设备上预先定义的热按钮。
- IMAPI CD-Burning COM Service：用 Image Mastering Applications Programming Interface 管理 CD 录制。
- Indexing Service：本地或远程计算机上文件的索引内容和属性，泄露信息。
- Messenger：信使服务。
- NetMeeting Remote Desktop Sharing：使授权用户能够通过使用 NetMeeting 跨企业 Intranet 远程访问此计算机。
- Network DDE：为在同一台计算机或不同计算机上运行的程序提供动态数据交换。
- Network DDE DSDM：管理动态数据交换(DDE)网络共享。
- Print Spooler：将文件加载到内存中以便迟后打印。
- Remote Desktop Help Session Manager：管理并控制远程协助。
- Remote Registry：使远程用户能修改此计算机上的注册表设置。
- Routing and Remote Access：在局域网及广域网环境中为企业提供路由服务。黑客利用路由服务刺探注册信息。
- Server：支持此计算机通过网络的文件、打印和命名管道共享。
- TCP/IP NetBIOS Helper：允许对 TCP/IP 上 NetBIOS(NetBT)服务及 NetBIOS 名称解析的支持。
- Telnet：允许远程用户登录到此计算机并运行程序。
- Terminal Services：允许多位用户连接并控制一台机器，并且在远程计算机上显示桌面和应用程序。
- Windows Image Acquisition(WIA)：为扫描仪和照相机提供图像捕获。

如果发现机器开启了一些很奇怪的服务，如 r_server，则必须马上停止该服务，因为这完全有可能是黑客使用控制程序的服务端。

3.4 关闭端口

先看一下如何查看本机打开的端口和 TCP/IP 端口的过滤。执行“开始”→“运行”命令，在打开的对话框中输入 cmd，然后输入命令 netstat -a，如图 3.5 所示。

1. 关闭自己的 139 端口，IPC 和 RPC 漏洞存在于此

开启 139 端口虽然可以提供共享服务，但是常常被攻击者利用进行攻击，如使用流光、SuperScan 等端口扫描工具可以扫描目标计算机的 139 端口，如果发现有漏洞，可以试图获取用户名和密码，这是非常危险的。关闭 139 端口的方法是在“网络连接”窗口中右击“本地连接”图标，在弹出的“本地连接属性”对话框中选中“Internet 协议(TCP/IP)”选项，单击“属性”按钮，在打开的“Internet 协议(TCP/IP)属性”对话框中单击“高级”按钮，进入“高级 TCP/IP 设置”对话框，在 WINS 选项卡中选中“禁用 TCP/IP 上的 NetBIOS”单选按钮，如图 3.6 所示。

```
C:\Documents and Settings\Administrator>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    PC-200811211103:epmap  PC-200811211103:0      LISTENING
  TCP    PC-200811211103:microsoft-ds  PC-200811211103:0      LISTENING
  TCP    PC-200811211103:912    PC-200811211103:0      LISTENING
  TCP    PC-200811211103:1025   PC-200811211103:0      LISTENING
  TCP    PC-200811211103:6059   PC-200811211103:0      LISTENING
  TCP    PC-200811211103:9010   PC-200811211103:0      LISTENING
  TCP    PC-200811211103:9011   PC-200811211103:0      LISTENING
  TCP    PC-200811211103:netbios-ssn  PC-200811211103:0      LISTENING
  TCP    PC-200811211103:1025   PC-200811211103:1349   ESTABLISHED
  TCP    PC-200811211103:1026   PC-200811211103:0      LISTENING
  TCP    PC-200811211103:1158   PC-200811211103:1025   CLOSE_WAIT
  TCP    PC-200811211103:1349   PC-200811211103:1025   ESTABLISHED
  TCP    PC-200811211103:netbios-ssn  PC-200811211103:0      LISTENING
  TCP    PC-200811211103:1350   219.238.235.94:http    ESTABLISHED
  TCP    PC-200811211103:netbios-ssn  PC-200811211103:0      LISTENING
  UDP    PC-200811211103:microsoft-ds  *:*
  UDP    PC-200811211103:isakmp  *:*
  UDP    PC-200811211103:4500   *:*
  UDP    PC-200811211103:ntp    *:*
```

图 3.5　开放的端口

2. 445 端口的关闭

445 端口和 139 端口是 IPC$入侵的主要通道,通过 445 端口可以偷偷共享硬盘,甚至会在悄无声息中将硬盘格式化。所以关闭 445 端口是非常必要的,可以封堵住 445 端口漏洞。修改注册表,添加一个键值 HKEY_LOCAL_MACHINE\System\Current ControlSet\Services\NetBT\Parameters,在右侧的窗口建立一个名称为 SMBDeviceEnabled 的 DWORD 值,类型为 REG_DWORD,键值为 0,如图 3.7 所示。

图 3.6　关闭 139 端口

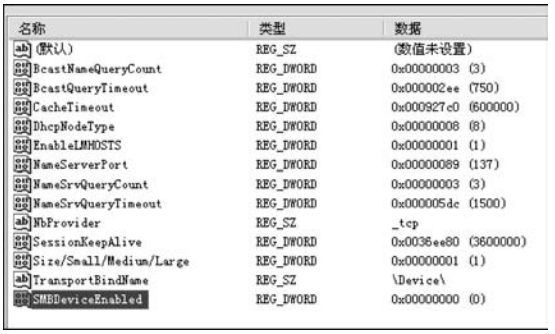


图 3.7　建立键值

3. 禁止终端服务远程控制、远程协助

“终端服务”是 Windows XP 在 Windows 2000 系统(Windows 2000 利用此服务实现远程的服务器托管)上遗留下来的一种服务形式,用户利用终端可以实现远程控制。“终端服务”和“远程协助”是有一定区别的,虽然实现的都是远程控制,但终端服务更注重用户的登录管理权限,它的每次连接都需要当前系统的一个具体登录 ID,且相互隔离,并独立于当前

计算机用户的邀请，可以独立、自由登录远程计算机。

在 Windows XP 系统下“终端服务”是默认启用的，也就是说，如果有人知道你计算机上的一个用户登录 ID，并且知道计算机的 IP，它就可以完全控制你的计算机。

在 Windows XP 系统中关闭“终端服务”的方法如下：右击“我的电脑”图标，从弹出的快捷菜单中选择“属性”命令，在“远程”选项卡中取消对“允许用户远程连接到此计算机”复选框的勾选，如图 3.8 所示。

在 Windows XP 上有一项“远程协助”功能，它允许用户在使用计算机发生困难时向 MSN 上的好友发出远程协助邀请帮助自己解决问题。

但是这个“远程协助”功能正是“冲击波”病毒所要攻击的 RPC(Remote Procedure Call)服务在 Windows XP 上的表现形式，建议用户不要使用该功能，使用前应该安装 Microsoft 提供的 RPC 漏洞工具和“冲击波”免疫程序。禁止“远程协助”的方法如下：右击“我的电脑”图标，在弹出的快捷菜单中选择“属性”命令，在“远程”选项卡中取消对“允许从这台计算机发送远程协助邀请”复选框的勾选。

4. 屏蔽闲置的端口

使用系统自带的“TCP/IP 筛选”服务就能够限制端口，方法如下：右击“网络连接”，从弹出的快捷菜单中选择“属性”命令，打开“网络连接属性”对话框，在“常规”选项卡中选中“Internet 协议(TCP/IP)”选项，然后单击“属性”按钮，在打开的“Internet 协议(TCP/IP)属性”对话框中单击“高级”按钮，在弹出的“高级 TCP/IP 设置”对话框中选择“选项”选项卡，再单击下面的“属性”按钮，最后弹出“TCP/IP 筛选”对话框，通过 “只允许”单选按钮，分别添加 TCP、UDP、IP 等网络协议允许的端口，如图 3.9 所示，然后添加需要的 TCP 和 UDP 端口就可以了。如果对端口不是很了解的话，不要轻易进行过滤，不然可能会导致一些程序无法使用。未提供各种服务的情况可以屏蔽掉所有的端口，这是最佳的安全防范形式，但是不适合初学者操作。

图 3.8　取消远程连接

图 3.9　网络协议允许的端口

3.5 使用 IP 安全策略关闭端口

(1) 打开控制面板,选择“管理工具”→“本地安全策略”,找到“IP 安全策略”,如图 3.10 所示。

(2) 右击右侧窗格的空白位置,在弹出的快捷菜单中选择“创建 IP 安全策略”命令,如图 3.11 所示。

图 3.10 找到“本地安全策略”中的“IP 安全策略”

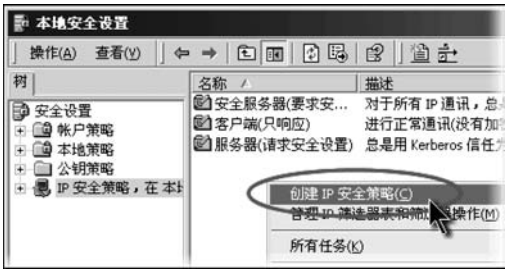


图 3.11 创建新的策略

在向导中单击“下一步”按钮,为新的安全策略命名,或者直接单击“下一步”按钮。

(3) 安全通信请求默认选中了“激活默认响应规则”复选框,取消勾选,如图 3.12 所示,再单击“下一步”按钮。

选中“编辑属性”复选框,单击“完成”按钮,如图 3.13 所示。

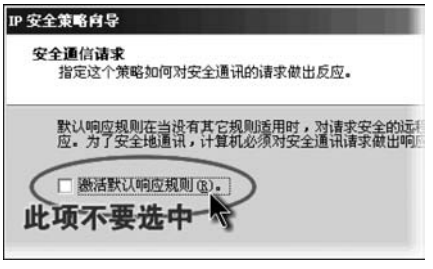


图 3.12 不要激活默认选中状态

(4) 在“新 IP 安全策略属性”对话框中查看“使用‘添加向导’”复选框有没有被选中,使之保持未选中状态,然后单击“添加”按钮,如图 3.14 所示。

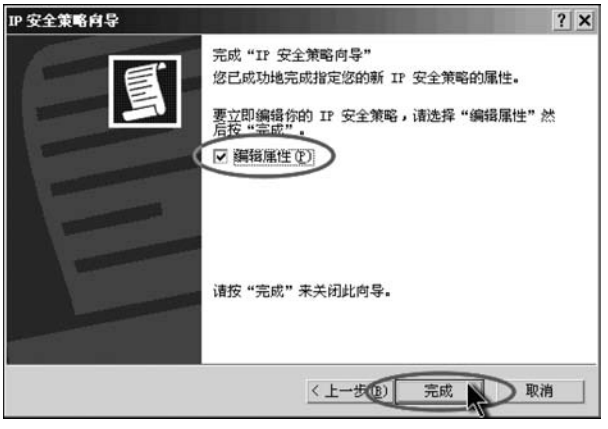


图 3.13 完成新策略添加

(5) 在“新规则属性”对话框中单击“添加”按钮，如图 3.15 所示。

图 3.14　单击“添加”按钮，添加新的连接规则

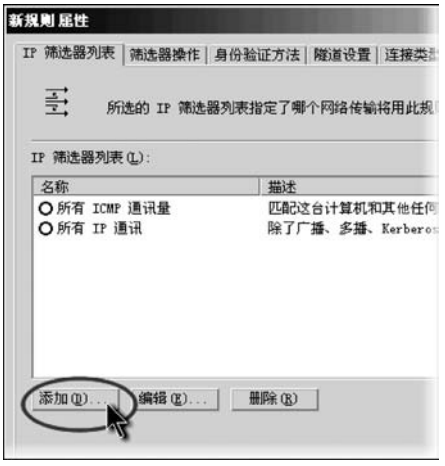


图 3.15　添加新的规则

(6) 在“IP 筛选器列表”对话框中取消“使用‘添加向导’”复选框的勾选，然后单击“添加”按钮，如图 3.16 所示。

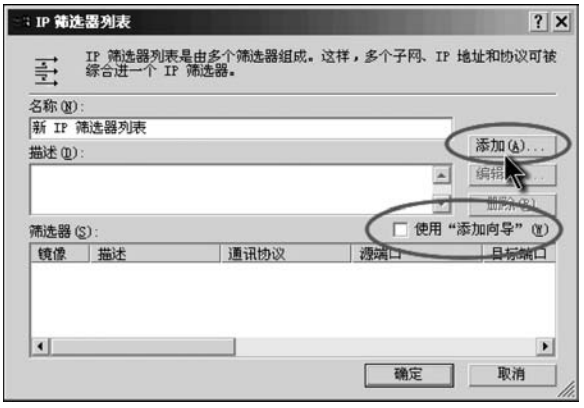


图 3.16　添加新的筛选器

(7) 在“筛选器属性”对话框中，在“源地址”下拉列表中选择“任何 IP 地址”，在“目标地址”下拉列表中选择“我的 IP 地址”，如图 3.17 所示。

(8) 选择“协议”选项卡，在“选择协议类型”下拉列表中选择 TCP，浅色的“设置 IP 协议端口”选项区域会变成可选，选中“到此端口”单选按钮，并在下方的文本框中输入 135，然后单击“确定”按钮，如图 3.18 所示。

(9) 回到“IP 筛选器列表”对话框，可以看到已经添加了一条策略，继续添加 TCP 137，139，445，593 端口和 UDP 135，139，445 端口。由于目前某些蠕虫病毒会扫描计算机的 TCP 1025，2745，3127，6129 端口，因此可以暂时添加这些端口的屏蔽策略，丢弃访问这些端口的数据包，不作响应，减少由此对上网造成的影响。单击“关闭”按钮，如图 3.19 所示。

图 3.17　筛选器属性

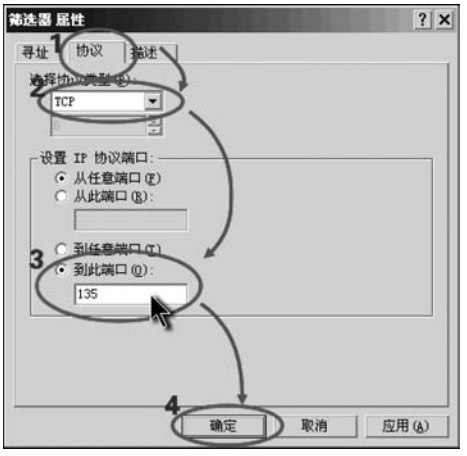


图 3.18　添加屏蔽 TCP 135(RPC)端口的筛选器

(10) 在“新规则属性”对话框中选择“新 IP 筛选器列表”,然后选择“筛选器操作”选项卡,如图 3.20 所示。

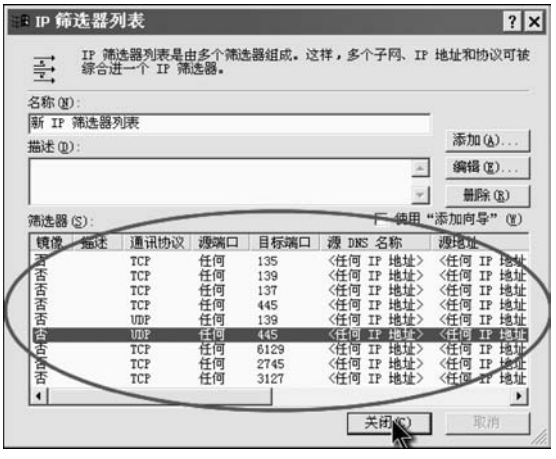


图 3.19　重复操作步骤,添加各端口筛选

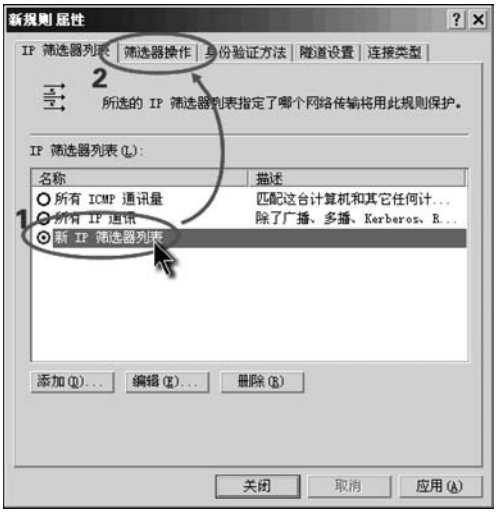


图 3.20　激活“新 IP 筛选器列表”

(11) 在“筛选器操作”选项卡中,取消勾选“使用‘添加向导’”复选框,然后单击“添加”按钮,如图 3.21 所示。

(12) 在“新筛选器操作属性”对话框中的“安全措施”选项卡中选择“阻止”单选按钮,然后单击“确定”按钮,如图 3.22 所示。

(13) 在“新规则属性”对话框中可以看到有一个“新筛选器操作”单选按钮,选中这个单选按钮,然后单击“关闭”按钮,如图 3.23 所示。

(14) 回到“新 IP 安全策略属性”对话框,单击“关闭”按钮,如图 3.24 所示。

(15) 返回到“本地安全设置”窗口,用右击新添加的 IP 安全策略,从弹出的快捷菜单中选择“指派”命令,如图 3.25 所示。

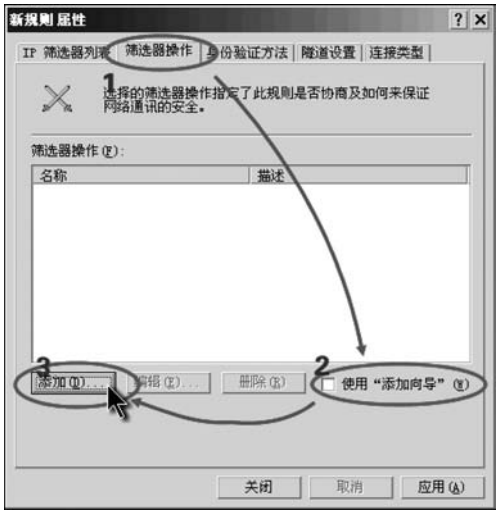


图 3.21　添加筛选器操作

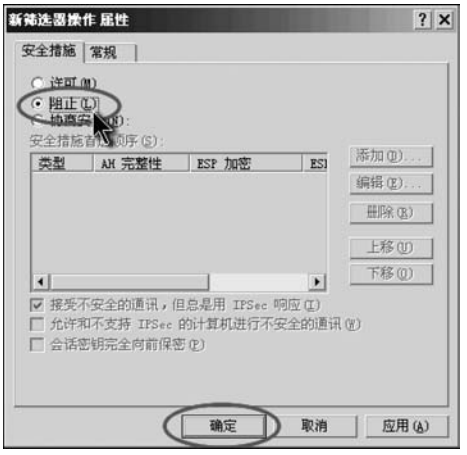


图 3.22　添加“阻止”操作

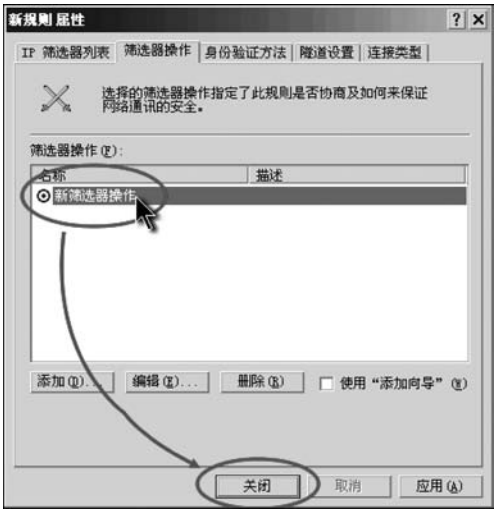


图 3.23　激活“新筛选器操作”

图 3.24　关闭“新 IP 安全策略属性”对话框

图 3.25　指派新的 IP 安全策略

3.6 本地安全策略设置

3.6.1 账户策略

在网络中,由于用户名和密码过于简单导致的安全性问题比较突出,有些人在攻击网络系统时也把破解管理员密码作为一个主要的攻击目标,关于账户策略,可以通过设置密码策略和账户锁定策略提高账户密码的安全级别。

打开控制面板,选择“管理工具”→“本地安全策略”→“账户策略”,然后双击“密码策略”,用于设置系统密码的安全规则,如图 3.26 所示。

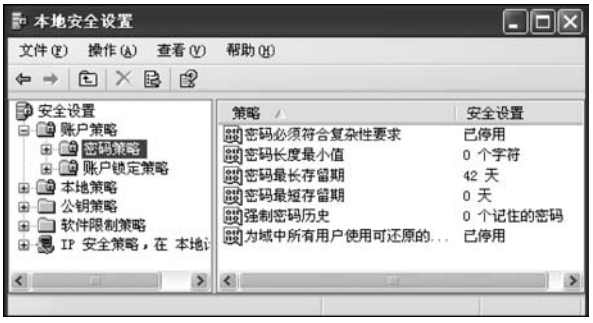


图 3.26 设置密码策略

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。双击其中每项,可按照需要改变密码特殊的设置。

(1) 双击“密码必须符合复杂性要求”策略,选择“启用”。选择控制面板中的“用户账户”选项,在弹出的对话框中选择一个用户,单击“创建密码”按钮,在弹出的设置密码窗口中输入密码,此时密码符合设置的密码要求。

(2) 双击“密码长度最小值”策略,在弹出的对话框中可设置被系统接纳的账户密码长度最小值。一般为达到较高安全性,密码长度最小值为 8。

(3) 双击“密码最长存留期”策略,设置系统要求的账户密码的最长使用期限为 42 天。设置密码自动存留期,用来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“密码最短存留期”策略,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,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存储密码”策略,在分别弹出的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。

3.6.2 账户锁定策略

为了防止他人进入计算机时反复猜测密码进行登录,可以锁定无效登录,当密码输入错误达设定次数后便锁定此账户,在一定时间内不能再以该账户登录。

选择“安全设置”→“账户策略”→“账户锁定策略”节点,打开“账户锁定阈值属性”对话

框，设置 3 次无效登录就锁住账号，如图 3.27 所示。

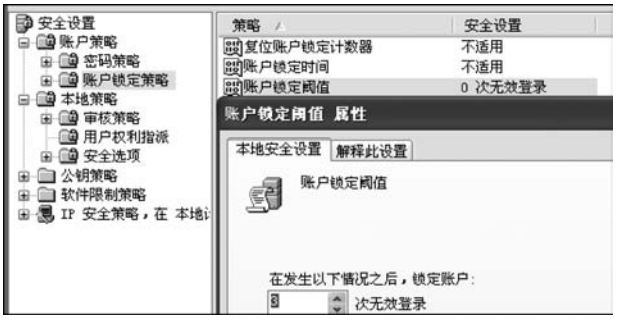


图 3.27　设置锁定阈值

“复位账户锁定计数器”和“账户锁定时间”策略的设置如图 3.28 所示。

图 3.28　锁定计数器与锁定时间

3.6.3　审核策略

审核策略可以帮助用户发现非法入侵者的一举一动，还可以作为用户将来追查黑客的依据。

选择“管理工具”→“安全设置”→“本地策略”→“审核策略”节点，把审核策略设置为图 3.29 所示内容。

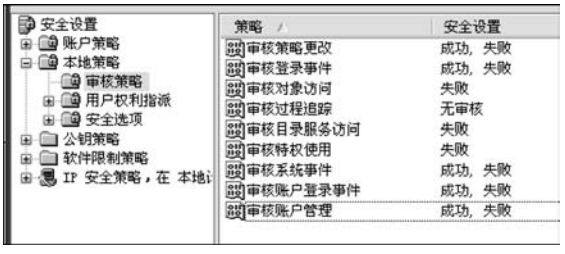


图 3.29　审核策略设置

然后进入控制面板，选择“管理工具”→“事件查看器”。

应用程序设置：右击“应用程序”，从弹出的快捷菜单中选择“属性”命令，将日志大小上限设置为 512KB，选中“不改写事件”单选按钮。

安全性设置：右击“安全性”，从弹出的快捷菜单中选择“属性”命令，将日志大小上限设置为 512KB，选中“不改写事件”单选按钮。

系统设置：右击“系统”，从弹出的快捷菜单中选择“属性”命令，将日志大小上限设置为512KB，选中“不改写事件”单选按钮。

3.6.4 安全选项

安全选项是作为增强 Windows 安全的最佳做法，同时也为攻击者设置更多的障碍，以减少对 Windows 的攻击的重要系统安全工具。在“本地策略”→“安全选项”中进行如下设置。

- 交互式登录：不显示最后的用户名(设置为启用)。
- 网络访问：不允许 SAM 账户的匿名枚举(设置为启用)。
- 网络访问：让 Everyone 权限应用于匿名用户(设置为关闭)。
- 网络访问：可匿名访问的共享(将后面的值删除)。
- 网络访问：可匿名访问的命名管道(将后面的值删除)。
- 网络访问：可远程访问的注册表路径(将后面的值删除)。
- 网络访问：可远程访问的注册表路径和子路径(将后面的值删除)。
- 网络访问：限制对命名管道和共享的匿名访问(将后面的值删除)。
- 网络安全：在下次更改密码时不存储 LAN 管理器的哈希值(设置为启用)。
- 关机：清除虚拟内存页面文件(设置为启用)。
- 关机：允许系统在未登录的情况下关闭(设置为关闭)。
- 账户：重命名系统管理员账户(确定一个新名字)。
- 账户：重命名来宾账户(确定一个新名字)。

3.6.5 用户权利指派策略

选择“管理工具”→“本地安全策略”→“本地策略”→“用户权利指派”节点，如图 3.30 所示。

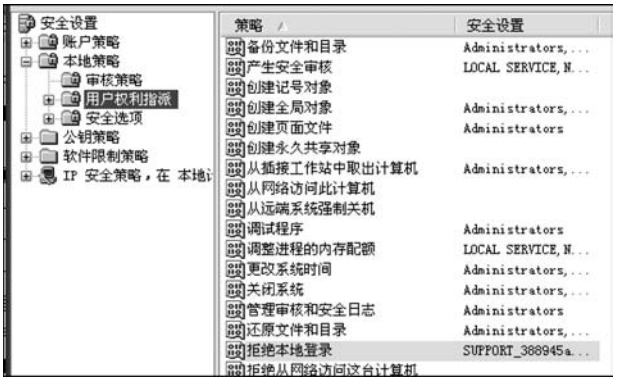


图 3.30 用户权利指派

- 从网络访问此计算机：一般默认有 5 个用户，删除 Administrators 外的其他 4 个。当然，接下来还得创建一个属于自己的 ID。
- 从远端系统强制关机：删除所有账户，一个都不留。
- 拒绝从网络访问这台计算机：将所有账户都删除。

- 从网络访问此计算机：如果不使用类似 3389 服务的话，Administrators 账户也可删除，其他全部账户都删除。
- 允许通过终端服务登录：删除所有账户，一个都不留。

3.7 用户策略

选择“管理工具”→“计算机管理”→“系统工具”→“本地用户和组”→“用户”节点，如图 3.31 所示。

图 3.31 用户策略

1. 停掉 Guest 账号

在“计算机管理”→“系统工具”→“本地用户和组”→“用户”节点中将 Guest 账号停用，任何时候都不允许 Guest 账号登录系统。为了保险起见，最好给 Guest 加一个复杂的密码。如果要启动 Guest 账号，一定要查看该账号的权限，只能以受限权限运行。

打开控制面板，选择“管理工具”→“计算机管理”→“系统工具”→“本地用户和组”→“用户”，右击 Guest 账户，从弹出的快捷菜单中选择“属性”命令，在弹出的对话框中选中“账户已停用”复选框。单击“确定”按钮，观察 Guest 前的图标变化，并再次使用 Guest 账户登录，记录显示的信息。

2. 限制不必要的用户数量

删除所有的 Duplicate User 账户、测试用账户、共享账户、普通部门账户等。用户组策略设置相应权限，并且经常检查系统的账户，删除已经不再使用的账户。这些账户很多时候都是黑客入侵系统的突破口，系统的账户越多，黑客得到合法用户的权限可能性也就越大。

3. 重命名 Administrator 账户

把系统 Administrator 账户重命名，Windows XP 的 Administrator 账户是不能停用的，这意味着别人可以一遍又一遍地尝试这个用户的密码。尽量把它伪装成普通用户，如改成 usera。

4. 创建一个陷阱用户

创建一个名为 Administrator 的本地用户，把它的权限设置为最低，什么事也干不了，并且加上一个超过 10 位的超级复杂密码。

3.8 安全模板设置

3.8.1 启用安全模板

启用前，先记录当前系统的账户策略和审核日志状态，以便与实验后的设置进行比较。

(1) 执行“开始”→“运行”命令，在弹出的对话框中输入 mmc，打开系统控制台。

(2) 执行“文件”→“添加/删除管理单元”菜单命令,在打开的“添加/删除管理单元”对话框中单击“添加”按钮,在弹出的窗口中分别选择“安全模板”和“安全配置和分析”,单击“添加”按钮后关闭窗口,并单击“确定”按钮,如图 3.32 所示。

(3) 此时系统控制台中根节点下添加了“安全模板”和“安全配置和分析”两个节点,展开“安全模板”节点,可以看到系统中存在的安全模板,如图 3.33 所示。右击模板名称,从弹出的快捷菜单中选择“设置描述”命令,可以看到该模板的相关信息。单击“打开”按钮,右侧窗口出现该模板的安全策略,双击每个安全策略可以看到其相关配置。

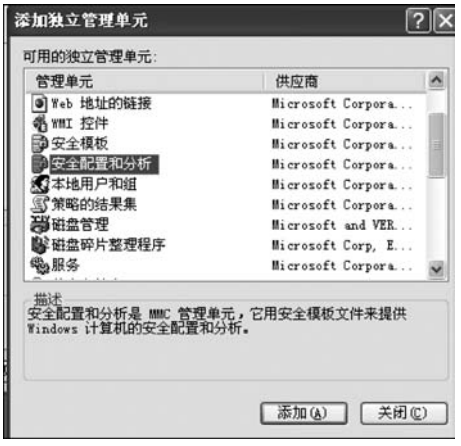


图 3.32 添加控制模块

图 3.33 安全模板

(4) 右击“安全配置和分析”节点,从弹出的快捷菜单中选择“打开数据库”命令,在弹出的对话框中输入预建安全数据库的名称,如命名为 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。

(5) 右击“安全配置和分析”节点,从弹出的快捷菜单中选择“立即分析计算机”命令,单击“确定”按钮,系统开始按照步骤(4)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。

(6) 右击“安全配置和分析”节点,从弹出的快捷菜单中选择“立即配置计算机”命令,按照步骤(4)所选的安全模板的要求对当前系统进行配置。

(7) 在实验报告中记录实验前系统的默认配置,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。

3.8.2 新建安全模板

(1) 展开“安全模板”节点,右击模板所在路径,从弹出的快捷菜单中选择“新加模板”命令,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”文本框中填入“自设模板”,查看新模板是否出现在模板列表中。

(2) 双击 mytem,在现实的安全策略列表中双击“账户策略”节点下的“密码策略”,可发现其中所有项均显示为“没有定义”,双击预设置的安全策略(如“密码长度最小值”)。

(3) 选中“在模板中定义这个策略设置”复选框,在文本框中输入密码的最小长度为 7。

(4) 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。

3.9 组策略设置

组策略是管理员为用户和计算机定义并控制程序、网络资源及操作系统行为的主要工具。通过组策略可以设置各种软件、计算机和用户策略。

3.9.1 关闭自动运行功能

(1) 执行“开始”→ “运行”命令,在打开的对话框中输入 gpedit.msc 并运行,打开“组策略”窗口。

(2) 选择“‘本地计算机’策略”→“计算机配置”→“管理模板” →“系统”节点,然后在右侧窗口中选择“设置”,双击“关闭自动播放”选项,如图 3.34 所示。

图 3.34 关闭自动播放

(3) 在弹出的对话框中选择“设置”选项卡,选中“已启用”单选按钮,然后在“关闭自动播放”下拉列表中选择“所有驱动器”,单击“确定”按钮,退出“组策略”窗口,如图 3.35 所示。

图 3.35 启动服务

在“用户配置”中同样也可以定制这个“关闭自动播放”服务,但“计算机配置”中的设置比“用户配置”中的设置范围更广,有助于多个用户都使用这样的设置。

3.9.2 禁止运行指定程序

系统启动时一些程序会在后台启动,这些程序通过"系统配置实用程序"(msconfig)的启动项无法阻止,操作起来非常不便,通过组策略则非常方便,这对减少系统资源占用非常有效。通过启用该策略并添加相应的应用程序就可以限制用户运行这些应用程序。具体步骤如下。

(1) 打开组策略对象编辑器,展开"'本地计算机'策略"→"计算机配置"→"管理模板"→"系统"节点,然后在右侧窗口中双击"不要运行指定的 Windows 应用程序"。

(2) 在弹出的对话框中双击禁止运行的程序,如 Wgatray.exe 即可。

当用户试图运行包含在不允许运行程序列表中的应用程序时,系统会提示警告信息。把不允许运行的应用程序复制到其他的目录和分区中仍然是不能运行的。要恢复指定的受限程序的运行,可以将"不要运行指定的 Windows 应用程序"策略设置为"未配置"或"已禁用",或者将指定的应用程序从不允许运行列表中删除(要求删除后列表不会成为空白的)。

这种方式只阻止用户运行从 Windows 资源管理器中启动的程序,对于由系统过程或其他过程启动的程序,并不能禁止其运行。该方式禁止应用程序的运行,其用户对象的作用范围是所有的用户,不仅仅是受限用户,Administrators 组中的账户甚至是内建的 Administrator 账户都将受到限制,因此给管理员带来了一定的不便。当管理员需要执行一个包含在不允许运行列表中的应用程序时,需要先通过组策略编辑器将该应用程序从不运行列表中删除,在程序运行完成后再将该程序添加到不允许运行程序列表中。需要注意的是,不要将组策略编辑器(gpedit.msc)添加到禁止运行程序列表中,否则会造成组策略的自锁,任何用户都将不能启动组策略编辑器,也就不能对设置的策略进行更改。

提示:如果没有禁止运行"命令提示符"程序的话,用户可以通过 cmd 命令从"命令提示符"运行被禁止的程序。例如,将记事本程序(notepad.exe)添加到不运行列表中,通过桌面和菜单运行该程序是被限制的,但是在"命令提示符"下运行 notepad 命令可以顺利地启动记事本程序。因此,要彻底禁止某个程序的运行,首先要将 cmd.exe 添加到不允许运行列表中。如果禁止程序后组策略无法使用,可以通过以下方法来恢复设置:重新启动计算机,在启动菜单出现时按 F8 键,在 Windows 高级选项菜单中选择"带命令行提示的安全模式"选项,然后在命令提示符下运行 mmc。

在打开的"控制台"窗口中执行"文件"→"添加/删除管理单元"菜单命令,单击"添加"按钮,选择"组策略对象编辑器",单击"添加"按钮,在弹出的"选择组策略对象"对话框中单击"完成"按钮,然后单击"关闭"按钮,再单击"确定"按钮,添加一个组策略控制台,接下来把原来的设置改回来,然后重新进入 Windows 即可。

3.9.3 防止菜单泄露隐私

在"开始"菜单中有一个"我最近的文档"菜单项,可以记录用户曾经访问过的文件。这个功能可以方便用户再次打开该文件,但别人也可通过此菜单访问用户最近打开的文档,安全起见,可屏蔽此项功能。具体操作步骤如下。

(1) 打开"组策略对象编辑器",展开"'本地计算机'策略"→"用户配置"→"管理模板"→"任务栏和「开始」菜单"节点。

(2) 分别在右侧窗口中双击“不要保留最近打开文档的记录”和“退出时清除最近打开的文档的记录”,打开目标策略属性设置对话框。

如果启用“退出时清除最近打开的文档的记录”设置,系统就会在用户注销时删除最近使用的文档文件的快捷方式。因此,用户登录时,“开始”菜单中的“我最近的文档”菜单总是空的。如果禁用或不配置此项设置,系统就会保留文档快捷方式,这样用户登录时,“我最近的文档”菜单中的内容与用户注销时一样。

提示:系统在“系统驱动器\Documents and Settings\用户名\我最近的文档”文件夹中的用户配置文件中保存文档快捷方式。

当没有选择“从‘开始’菜单删除最近的项目菜单”和“不要保留最近打开文档的记录”策略的任何一个相关设置时,此项设置才能使用。

3.10 文件加密系统

每个人都有一些不希望被别人看到的东西,如学习计划、情书等,大家都喜欢把它们放在一个文件夹里,采用 Windows 自带的文件夹加密功能实现对文件加密。NTFS 是 Windows NT 以上版本支持的一种提供安全性、可靠性的高级文件系统。在 Windows 2000 和 Windows XP 中,NTFS 提供诸如文件和文件夹加密的高级功能。

3.10.1 加密文件或文件夹

(1) 执行“开始”→“所有程序”→“附件”→“Windows 资源管理器”命令,打开 Windows 资源管理器。

(2) 右击要加密的文件或文件夹,从弹出的快捷菜单中选择“属性”命令。

(3) 在弹出的对话框中的“常规”选项卡上单击“高级”按钮,在打开的“高级属性”对话框中选中“加密内容以便保护数据”复选框,如图 3.36 所示。

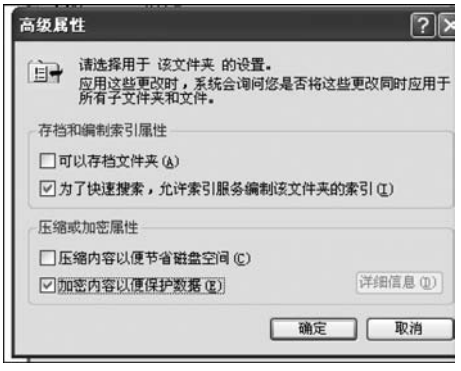


图 3.36 加密选项

在加密过程中还要注意以下几点。

(1) 只可以加密 NTFS 分区卷上的文件和文件夹,对 FAT 分区卷上的文件和文件夹无效。

(2) 被压缩的文件或文件夹也可以加密。如果要加密一个压缩文件或文件夹,则该文件或文件夹将被解压。

(3) 无法加密标记为“系统”属性的文件,并且位于操作系统根目录结构中的文件也无法加密。

(4) 在加密文件夹时,系统将询问是否要同时加密它的子文件夹。如果单击“是”按钮,那么它的子文件夹也会被加密,以后所有添加进文件夹中的文件和子文件夹都将在添加时自动加密。

加密后用不同用户登录计算机,查看加密文件是否能够打开。

3.10.2 备份加密用户的证书

用户对文件加密后,在重装系统或删除用户前一定要备份加密用户的证书,否则重装系统或删除用户后加密文件将无法被访问。

图 3.37 添加证书模块

(1) 以加密用户账户登录计算机。

(2) 执行“开始”→“运行”命令,在弹出的对话框中输入 mmc,然后单击“确定”按钮。

(3) 在“控制台”窗口执行“文件”→“添加/删除管理单元”菜单命令,在打开的“添加/删除管理单元”对话框中单击“添加”按钮。

(4) 打开“添加独立管理单元”对话框,在“可用的独立管理单元”列表框中选择“证书”,然后单击“添加”按钮,如图 3.37 所示。

(5) 在弹出的对话框中选中“我的用户账户”单选按钮,然后单击“完成”按钮。

(6) 单击“关闭”按钮,然后单击“确定”按钮。

(7) 展开“证书-当前用户”→“个人”→“证书”节点,如图 3.38 所示。

图 3.38 显示加密证书

(8) 右击“预期目的”栏中显示“加密文件系统”字样的证书。

(9) 从弹出的快捷菜单中选择“所有任务”→“导出”命令,如图 3.39 所示。

图 3.39 导出证书

(10) 按照证书导出向导的指示将证书及相关的私钥以 PFX 文件格式导出。注意:推荐使用“导出私钥”方式导出,如图 3.40 所示,这样可以保证证书受密码保护,以防别人盗用。另外,证书只能保存到用户有读写权限的目录下。

(11) 保存好证书,将 PFX 文件保存好。以后重装系统之后无论在哪个用户账户下只要双击这个证书文件,导入这个私人证书就可以访问 NTFS 系统下由该证书的原用户加密的文件夹。

最后要提一下,这个证书还可以实现以下用途。

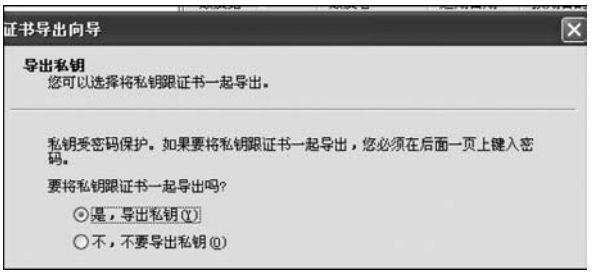


图 3.40　导出私钥

(1) 给予不同用户访问加密文件夹的权限。

将证书按“导出私钥”方式导出，发给需要访问这个文件夹的本机其他用户。然后由其他用户登录，导入该证书，实现对这个文件夹的访问。

(2) 在其他 Windows XP 机器上对用“备份恢复”程序备份的以前的加密文件夹恢复访问权限。

将加密文件夹用“备份恢复”程序备份，然后把生成的 Backup.bkf 连同这个证书复制到另外一台 Windows XP 机器上，用“备份恢复”程序将它恢复出来(注意：只能恢复到 NTFS 分区)。然后导入证书，即可访问恢复出来的文件。

3.11　文件和数据的备份

为了保护服务器，用户应该安排对所有数据进行定期备份。建议安排对所有数据(包括服务器的系统状态数据)进行每周普通备份。普通备份将复制用户选择的所有文件，并将每个文件标记为已备份。此外，还建议安排进行每周差异备份。差异备份复制自上次普通备份以来创建和更改的文件。

3.11.1　安排进行每周普通备份

(1) 执行“开始”→“运行”命令，在打开的对话框中输入 ntbackup，然后单击“确定”按钮，弹出“备份或还原向导”对话框，单击“下一步”按钮。

(2) 在“备份或还原”页面中确保已选中“备份文件和设置”单选按钮，然后单击“下一步”按钮。在“要备份的内容”页面中选中“让我选择要备份的内容”单选按钮，然后单击“下一步”按钮。

(3) 在“要备份的项目”页面中单击项目以展开其内容，勾选包含应该定期备份的数据的所有设备或文件夹的复选框，然后单击“下一步”按钮，如图 3.41 所示。

(4) 在“备份类型、目标和名称”页面中的“选择保存备份的位置”下拉列表中选择或单击“浏览”按钮以选择保存备份的位置。在“键入这个备份的名称”文本框中为该备份输入一个描述性名称，然后单击“下一步”按钮，如图 3.42 所示。

(5) 在“正在完成备份或还原向导”页面中单击“高级”按钮，在“备份类型”页面中的“选择要备份的类型”下拉列表中选择“正常”选项，然后单击“下一步”按钮，如图 3.43 所示。

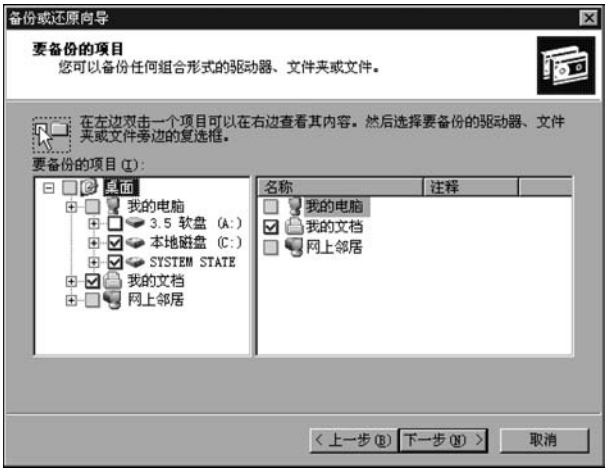


图 3.41　要备份的项目

图 3.42　备份类型、目标和名称

图 3.43　备份类型

(6) 在“如何备份”页面中勾选“备份后验证数据”复选框，然后单击“下一步”按钮。在“备份选项”页面中确保选中“将这个备份附加到现有备份”单选按钮，然后单击“下一步”按钮，如图 3.44 所示。

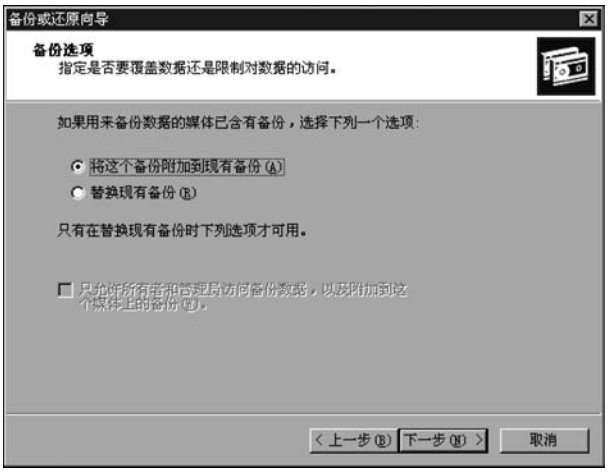


图 3.44　备份选项

(7) 在“备份时间”页面中的“什么时候执行备份?”下选中“以后”单选按钮，在“计划项”选项区域中的“作业名”文本框中输入描述性名称，然后单击“设定备份计划”按钮，如图 3.45 所示。

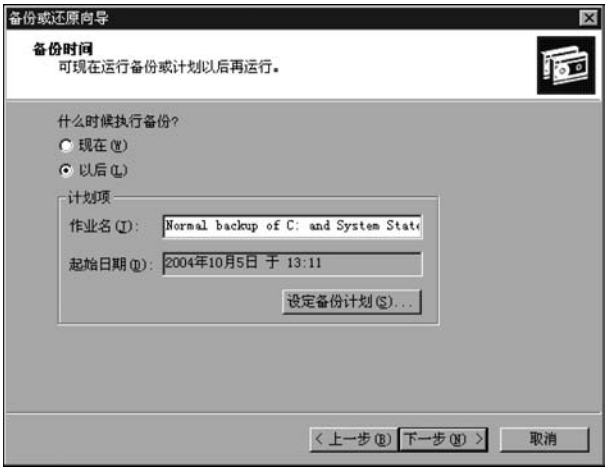


图 3.45　备份时间

(8) 在“计划作业”对话框中的“计划任务”下拉列表中选择“每周”，在“开始时间”调节框中使用向上和向下箭头键设置开始备份的适当时间。单击“高级”按钮以指定计划任务的开始日期和结束日期，或指定计划任务是否按照特定时间间隔重复运行。在“每周计划任务”选项区域中，根据需要选择一天或几天以创建备份，然后单击“确定”按钮，如图 3.46 所示。

(9) 在“设置账户信息”对话框中的“运行方式”文本框中输入域、工作组和已授权执行备份和还原操作的账户的用户名，使用 DOMAIN\username 或 WORKGROUP\username

格式。在“密码”文本框中输入用户账户的密码。在“确认密码”文本框中再次输入密码,然后单击“确定”按钮,如图 3.47 所示。在“完成备份或还原向导”对话框中确认设置,然后单击“完成”按钮。

图 3.46 计划作业

图 3.47 设置账户信息

3.11.2 安排进行每周差异备份

操作步骤与普通备份基本相同,只是在“备份类型”页面的“选择要备份的类型”下拉列表框中选择“差异”,然后单击“下一步”按钮,如图 3.48 所示。

图 3.48 差异备份

3.11.3 从备份恢复数据

(1) 运行“开始”→“运行”命令,在打开的对话框中输入 ntbackup,然后单击“确定”按钮,弹出“备份或还原向导”对话框,单击“下一步”按钮。

(2) 在“备份或还原”页面中选中“还原文件和设置”单选按钮，然后单击“下一步”按钮。在“还原项目”页面中单击项目以展开其内容，选择包含要还原的数据的所有设备或文件夹，然后单击“下一步”按钮，如图 3.49 所示。

图 3.49　还原项目

(3) 在“正在完成备份或还原向导”页面中，如果要更改任何高级还原选项，如还原安全设置和交接点数据，则单击“高级”按钮。完成设置高级还原选项后，单击“确定”按钮，验证是否所有设置都正确，然后单击“完成”按钮。

实验思考题

1. 计算机中常用服务都使用了哪些端口？
2. 如何建立一个相对比较安全的共享？
3. 如何根据网络环境的不同快速调整安全策略？
4. 加密证书如何保存才会安全？
5. 计算机中哪些数据需要定期备份？