



从不同的角度看安全

目录

01

系统加固

Windows操作系统加固

Linux操作系统加固

02

中间件加固

IIS加固

Apache加固

Nginx加固

03

数据库加固

Mysql加固

Mongodb加固



windows 安全加固

目录

01

windows系统基本操作

02

windows系统加固

windows系统基本操作

windows常见目录

system32

存放系统配置文件

SysWOW64

Windows操作系统的子系统

Config/SAM

存放windows帐号和密码

etc/hosts

DNS解析文件

Program files/ Program files (x86)

64位系统安装在Windows操作系统的子系统,32位下会安装在x86下

Perflogs

日志目录

windows常用系统命令

命令	说明
ver	查看系统版本
hostname	查看主机名
ipconfig /all	查看网络配置
net user/localgroup/share/config	查看用户/用户组/共享/当前运行可配置服务
at	建立或查看系统作业
netstat	查看开放端口
secpol.msc	查看和修改本地安全设置
services.msc	查看和修改服务
eventvwr.msc	查看日志
regedit	打开注册表
whoami	查看当前操作用户的用户名

windows常见端口

端口	说明
80/8080/8081	HTTP协议代理服务器常用端口号
443	HTTPS协议代理服务器常用端口号
21	FTP(文件传输协议)协议代理服务器常用端口号
23	Telnet(远程登录)协议代理服务器常用端口号
22	SSH（安全登录）、SCP（文件传输）
1521	Oracle 数据库
1433	MS SQL SERVER数据库
1080	QQ
3306	Mysql数据库
25	SMTP（简单邮件传输协议）

net 命令的使用

创建（空密码）账户abc	net user abc /add
查看账户abc的详细信息	net user abc
删除账户abc	net user abc /del
创建普通账户abc，密码为123	net user abc 123/add
把abc用户加入管理员组	net localgroup administrators abc /add
把abc用户退出管理员组	net localgroup administrators abc /del
启用[停用]abc账户	net user abc /active:yes[no]
新建[删除]组admin	net localgroup admin /add[del]
查看本地开启的共享	net share
常看开启哪些端口	netstat

windows系统加固

账号安全是计算机系统安全的第一关，如果计算机系统账号被盗用，那么计算机将非常危险，入侵者可以任意控制计算机系统，如果计算机中存在着重要的机密文件，或者银行卡号和密码，那么损失会非常严重。

账号及安全策略

账号安全设置

设置方法：“开始” — “运行” 输入secpol.msc（控制面板——管理工具）

立即生效：gpupdate /force

账号策略

密码必须符合复杂性要求：启用

密码长度最小值 8个字符

密码最长使用期限： 30天

强制密码历史： 3个记住的密码

账号锁定

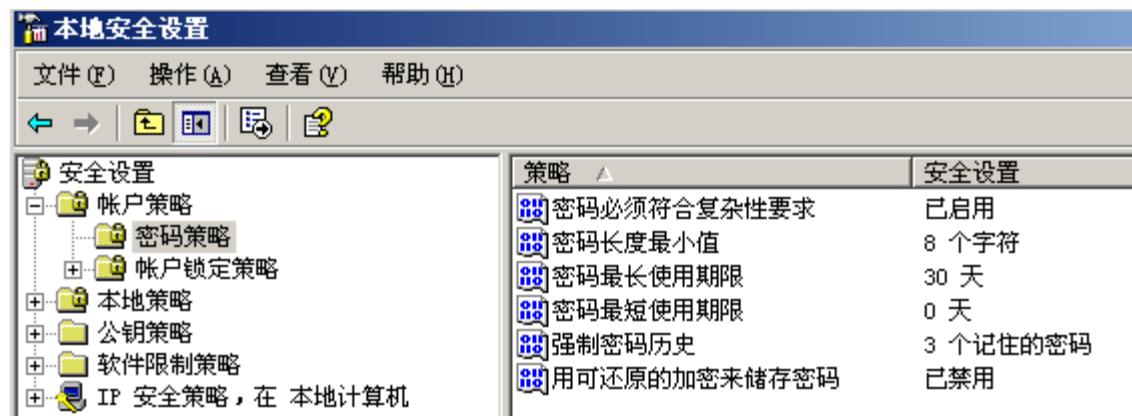
帐户锁定阈值： 3次无效登陆

帐户锁定时间： 30分钟

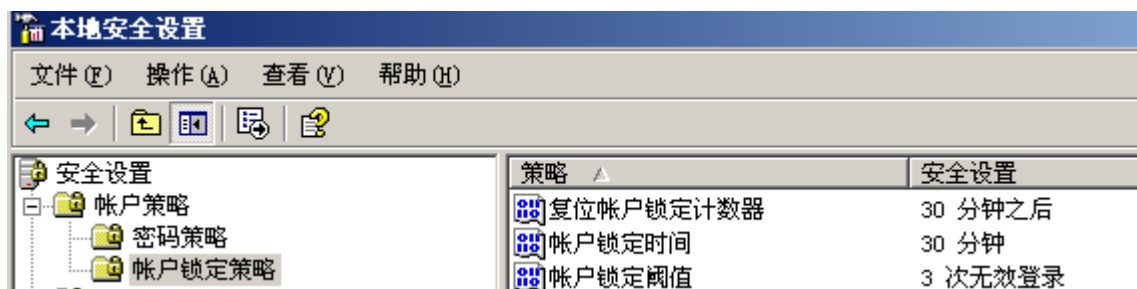
复位帐户锁定计数器：30分钟之后

账号及安全策略

账户密码策略



账户锁定策略



禁用Guest账户权限

“我的电脑”右击“管理”打开—计算机管理—本地用户和组—用户—Guest—右键—属性—常规—选择“账户已禁用”。

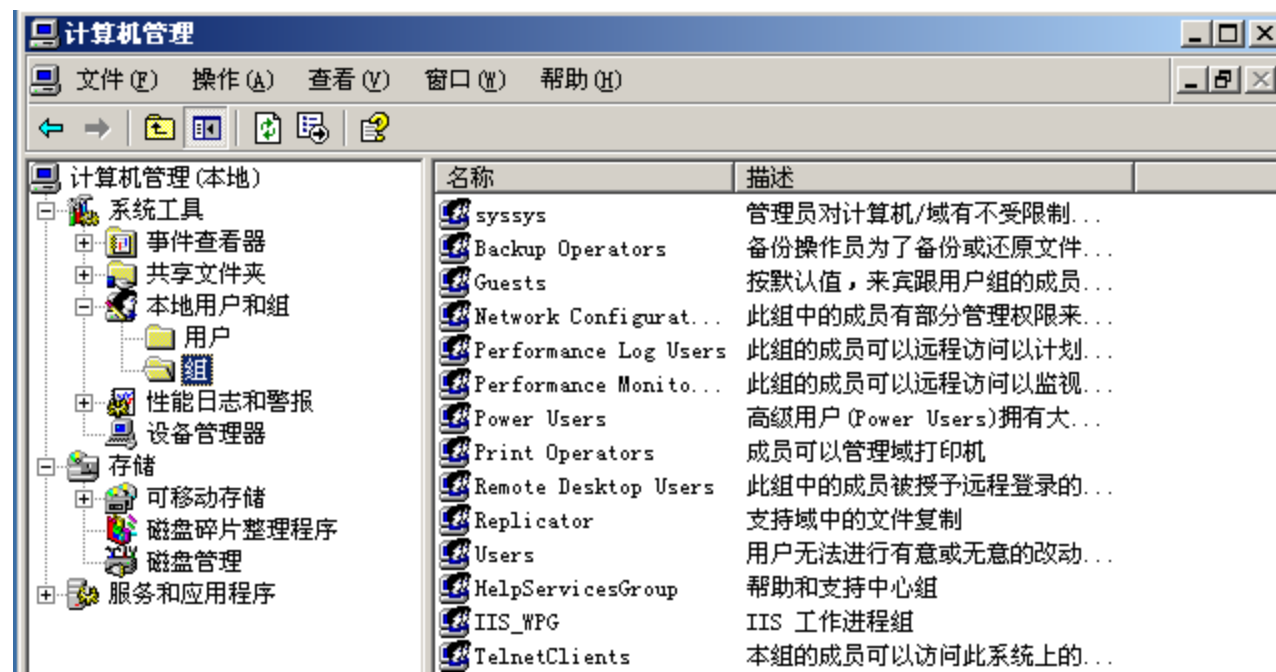
`net user guest /active:no`



Administartor账号、组重命名

Administartor账号、组重命名，可增加账号安全性

wmic useraccount where name='Administrator' call Rename admin

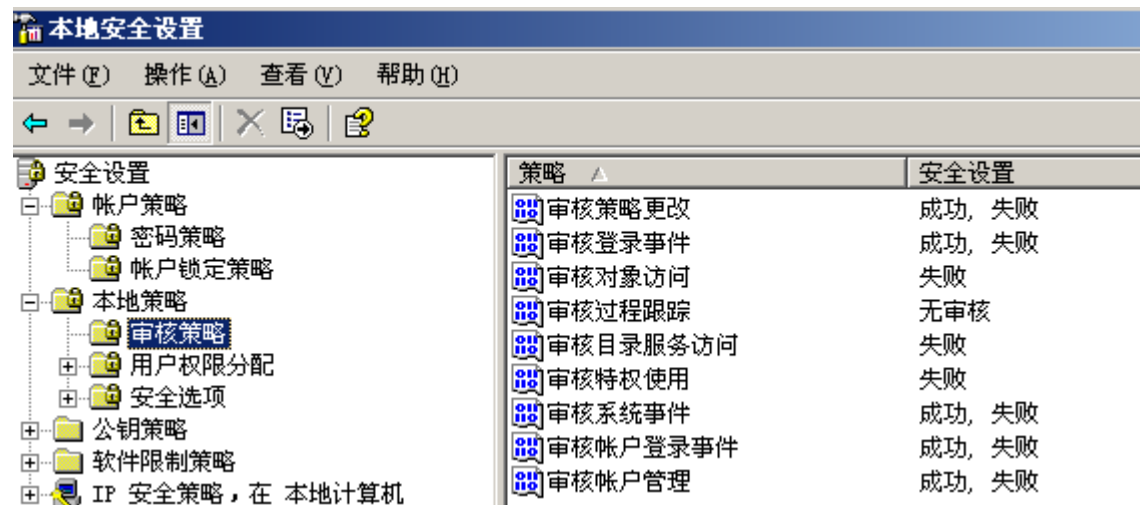


日志及审核策略

对重要事件进行审核记录，方便日后出现问题时查找问题根源。

审核策略：

审核策略更改	成功，失败
审核登陆事件	成功，失败
审核对象访问	失败
审核目录服务访问	失败
审核特权使用	失败
审核系统事件	成功，失败
审核账户登陆事件	成功，失败
审核帐户管理	成功，失败



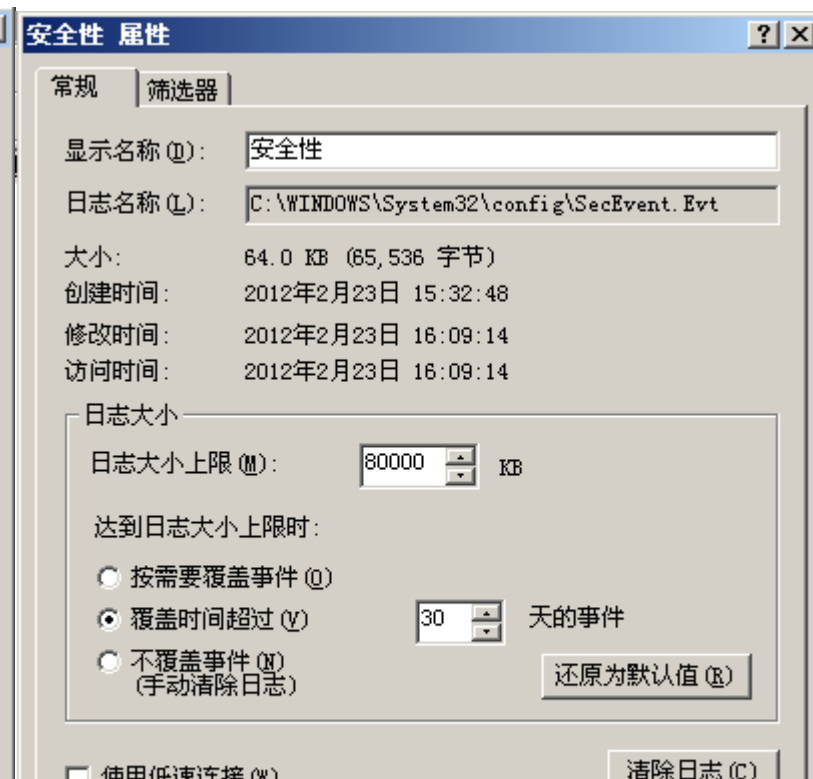
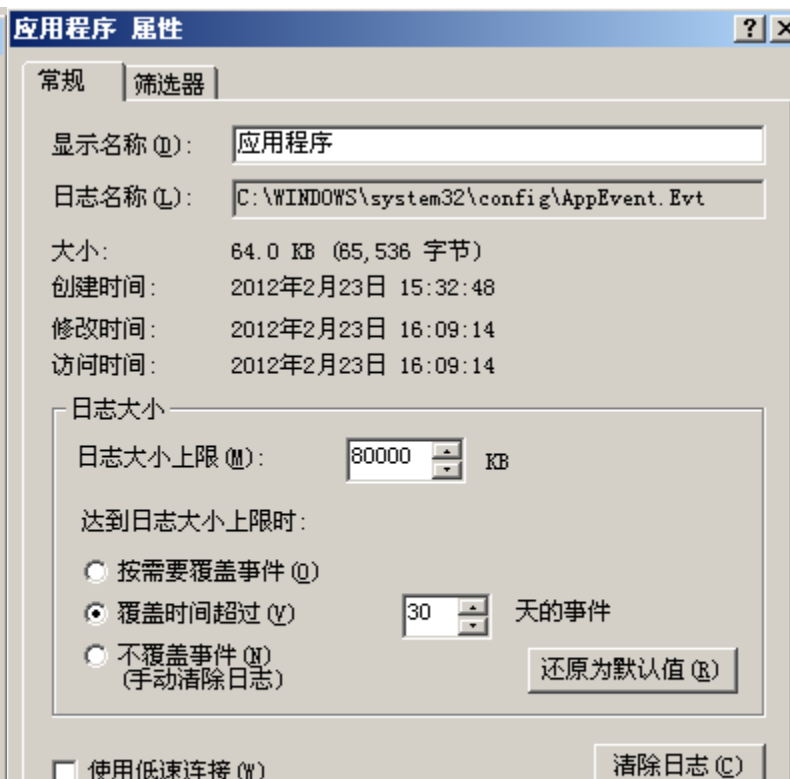
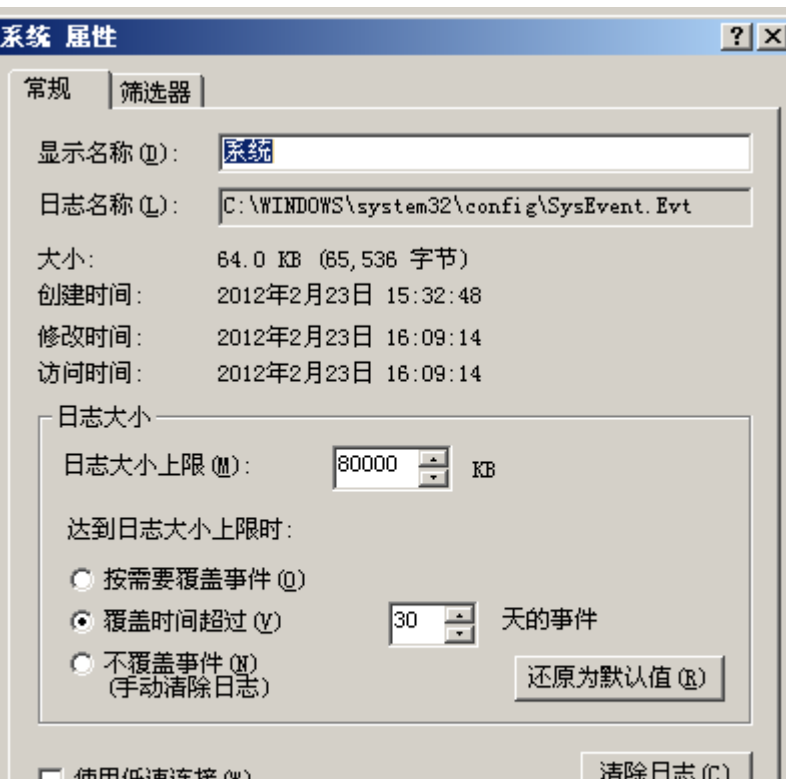
调整事件日志的大小及覆盖策略

日志安全设置

设置方法：“开始” — “运行” 输入eventvwr.msc

增大日志大小，避免由于日志文件容量过小导致重要日志记录遗漏

日志类型	日志大小	覆盖策略
应用程序	80000KB	覆盖早于30天的日志
安全日志	80000KB	覆盖早于30天的日志
系统日志	80000KB	覆盖早于30天的日志




在一个完整的信息系统里面，日志系统是一个非常重要的功能组成部分。它可以记录下系统所产生的所有行为，并按照某种规范表达出来。我们可以使用日志系统所记录的信息为系统进行排错，优化系统的性能，或者根据这些信息调整系统的行为。在安全领域，日志系统的重要地位尤甚，可以说是安全审计方面最主要的工具之一。

安全选项策略设置

本地安全策略->本地策略->安全选项


Microsoft 网络服务器：当登录时间用完时自动注销用户（启用）

目的：可以避免用户在不适合的时间登录到系统,或者用户登录到系统后忘记退出登录

 Microsoft 网络服务器：当登录时间用完时自动注销用户 已启用


Microsoft 网络服务器：在挂起会话之前所需的空闲时间（小于等于30分钟）

目的：设置挂起会话之前所需的空闲时间为30分钟

 Microsoft 网络服务器：在挂起会话之前所需的空闲时间 30 分钟


Microsoft 网络客户端：发送未加密的密码到第三方SMB服务器（禁用）

目的：禁止发送未加密的密码到第三方SMB服务器

 Microsoft 网络客户端：发送未加密的密码到第三方 SMB 服务器 已禁用

故障恢复控制台:允许对所有驱动器和文件夹进行软盘复制和访问（禁用）


目的：禁止它访问硬盘驱动器上的所有文件和目录。它仅允许访问每个卷的根目录%systemroot%目录及子目录，即使是这样它还限制不允许把硬盘驱动器上的文件拷贝到软盘上

 故障恢复控制台：允许对所有驱动器和文件夹进行软盘复制和访问 已禁用

安全选项策略设置

故障恢复控制台:允许自动系统管理级登录（禁用）

目的：恢复控制台是Windows 2003的一个新特性，它在一个不能启动的系统上给出一个受限的命令访问界面。可能会导致任何可以重起系统的人绕过账号口令限制和其它安全设置而访问系统

 故障恢复控制台：允许自动系统管理级登录 已禁用

关机：清除虚拟内存页面文件（启用）

目的：某些第三方的程序可能把一些没有的加密的密码存在内存中，页面文件中也可能含有另外一些敏感的资料。关机的时候清除页面文件，防止造成意外的信息泄漏

 关机：清除虚拟内存页面文件 已启用


关机：允许系统在未登录前关机（禁用）

目的：在未登录前不能关闭计算机

 关机：允许系统在未登录前关机 已禁用

交互式登录：不显示上次用户名（启用）

目的：登陆时不显示上次用户名，防止暴露用户名。

 交互式登录：不显示上次用户名 已启用

交互式登录：不需要按Ctrl+Alt+Del（禁用）


目的：登录时需要按CTRL+ALT+DEL

 交互式登录：不需要按 CTRL+ALT+DEL 已禁用

安全选项策略设置


交互式登录：可被缓存的前次登录个数（设置缓存数为0，此项对域服务器无效。）

目的：登陆时不显示上次的用户名，防止暴露用户名


 交互式登录：可被缓存的前次登录个数（在域控制器不可用的情况下） 0 次登录

网络访问：不允许SAM帐户和共享的匿名枚举（启用）

目的：禁止使用匿名用户空连接枚举系统敏感信息

 网络访问：不允许 SAM 帐户和共享的匿名枚举 已启用


网络访问：不允许为网络身份验证储存凭证或 .NET passports(启用)

 网络访问：不允许为网络身份验证储存凭证或 .NET Passports 已启用

审核：如果无法记录安全审核则立即关闭系统（启用）

 审核：如果无法记录安全审核则立即关闭系统 已启用

审核：对全局系统对象的访问进行审核（启用）

 审核：对全局系统对象的访问进行审核 已启用

安全选项策略设置

网络访问：本地账户的共享和安全模式：仅来宾--本地账户以来宾用户身份验证



网络访问：本地帐户的共享和安全模式

仅来宾 - 本地用...

网络访问：可匿名访问的共享（全部删除）



网络访问：可匿名访问的共享

网络访问：可匿名访问的命名管道（全部删除）



网络访问：可匿名访问的命名管道

网络访问：可远程访问的注册表路径（全部删除）



网络访问：可远程访问的注册表路径

网络访问：可远程访问的注册表路径和子路径（全部删除）



网络访问：可远程访问的注册表路径和子路径

用户权限策略设置

“通过终端服务拒绝登陆” 中加入Guests、User组

 通过终端服务拒绝登录


Users, Guests

“通过终端服务允许登陆” 中只加入Administrators组

 通过终端服务允许登录


Administrators

“从网络访问此计算机” 中删除PowerUsers和BackupOperators

 从网络访问此计算机

Users, IWAM_ZPK-...

“拒绝本地登录” 中添加web和guest用户

 拒绝本地登录

ZPK-SL65Z3PFRYU...

文件系统又被称作文件管理系统，它是指操作系统中负责管理和存储文件信息的软件机构。文件系统由与文件管理有关的软件、被管理的文件以及实施文件管理所需的数据结构这三部分构成。

从系统角度来看，文件系统是对文件存储器空间进行组织和分配，负责文件的存储并对存入的文件进行保护和检索的系统。具体地说，它负责为用户建立文件，存入、读出、修改、转储文件，控制文件的存取，当用户不再使用时撤销文件等。

Windows权限的继承性、累加性、优先性、交叉性和四项基本原则

Windows NT以后的文件，及文件夹共享设置有以下特性：继承性、累加性、优先性、交叉性。

- 继承性：下级的目录在没有经过重新设置之前，是拥有上一级目录权限设置的。
- 累加性：是说如一个组GROUP1中有两个用户USER1、USER2，他们同时对某文件或目录的访问权限分别为“读取”和“写入”，那么组GROUP1对该文件或目录的访问权限就为USER1和USER2的访问权限之和。
- 优先性：权限的这一特性又包含两种子特性，其一是文件的访问权限优先目录的权限，也就是说文件权限可以越过目录的权限，不顾上一级文件夹的设置。另一特性就是“拒绝”权限优先其它权限，也就是说“拒绝”权限可以越过其它所有其它权限，一旦选择了“拒绝”权限，则其它权限也就不能取任何作用，相当于没有设置。
- 交叉性：指当同一文件夹在为某一用户设置了共享权限的同时又为用户设置了该文件夹的访问权限，且所设权限不一致时，它的取舍原则是取两个权限的交集，也即最严格、最小的那种权限。如目录A为用户USER1设置的共享权限为“只读”，同时目录A为用户USER1设置的访问权限为“完全控制”，那用户USER1的最终访问权限为“只读”。

权限设置

系统分区C盘

administrator、system完全控制

C:\Documents and Settings\

administrator、system完全控制

C:\windows\system32\

administrator读写

C:\progrn files

为Common File目录之外的所有目录赋予Administrators 和SYSTEM 完全控制

C:\windows

系统管理员完全控制、system拒绝(继承)

C:\windows\system32

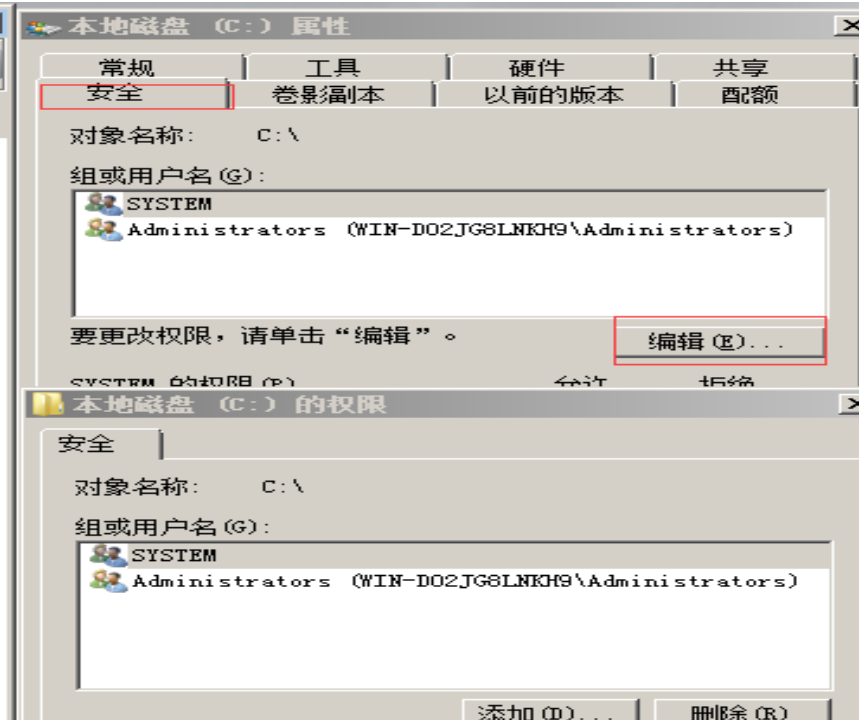
其关键程序只允许administrator完全控制

C:\Inetpub\

administrator、system完全控制，必要时可以删除该目录

网站目录所在磁盘

administrator、system完全控制

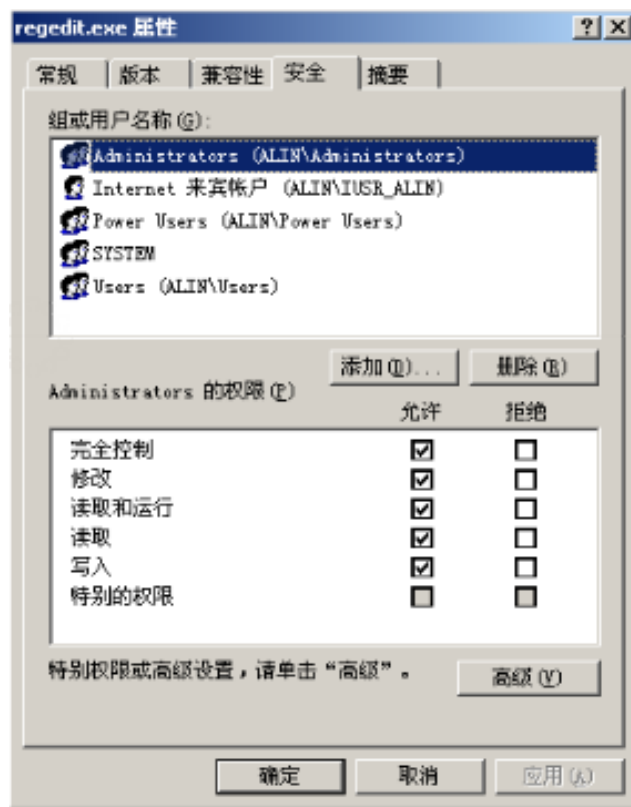


通过注册表，用户可以轻易地添加、删除、修改windows系统内的软件配置信息或硬件驱动程序，这不仅方便了用户对系统软硬件的工作状态进行适时的调整，于此同时注册表也是入侵者攻击的目标，通过注册表也可称为入侵者攻击的目标，通过注册表种植木马、修改软件信息，甚至删除、停用或改变硬件的工作状态。

HKEY_LOCAL_MACHINE	包含关于本地计算机系统的信息，包括硬件和操作系统数据
HKEY_LOCAL_ROOT	包含各种OLE技术使用的信息技术和文件类别关联数据
HKEY_LOCAL_USER	包含环境变量、桌面设置、网络连接、打印机和程序首选项
HKEY_LOCAL_USERS	包含关于动态加载的用户配置文件和默认的配置文件的信息。有些信息和HKEY_CURRENT_USER交叉出现
HKEY_CURRENT_CONFIG	包含在启动时由本地计算机系统使用的硬件配置文件的相关信息

注册表安全设置

利用文件管理器对regedit.exe文件设置成只允许管理员能使用命令访问修改注册表，其他用户只能读取，但不能修改这样就可以防止非法用户恶意修改注册表。



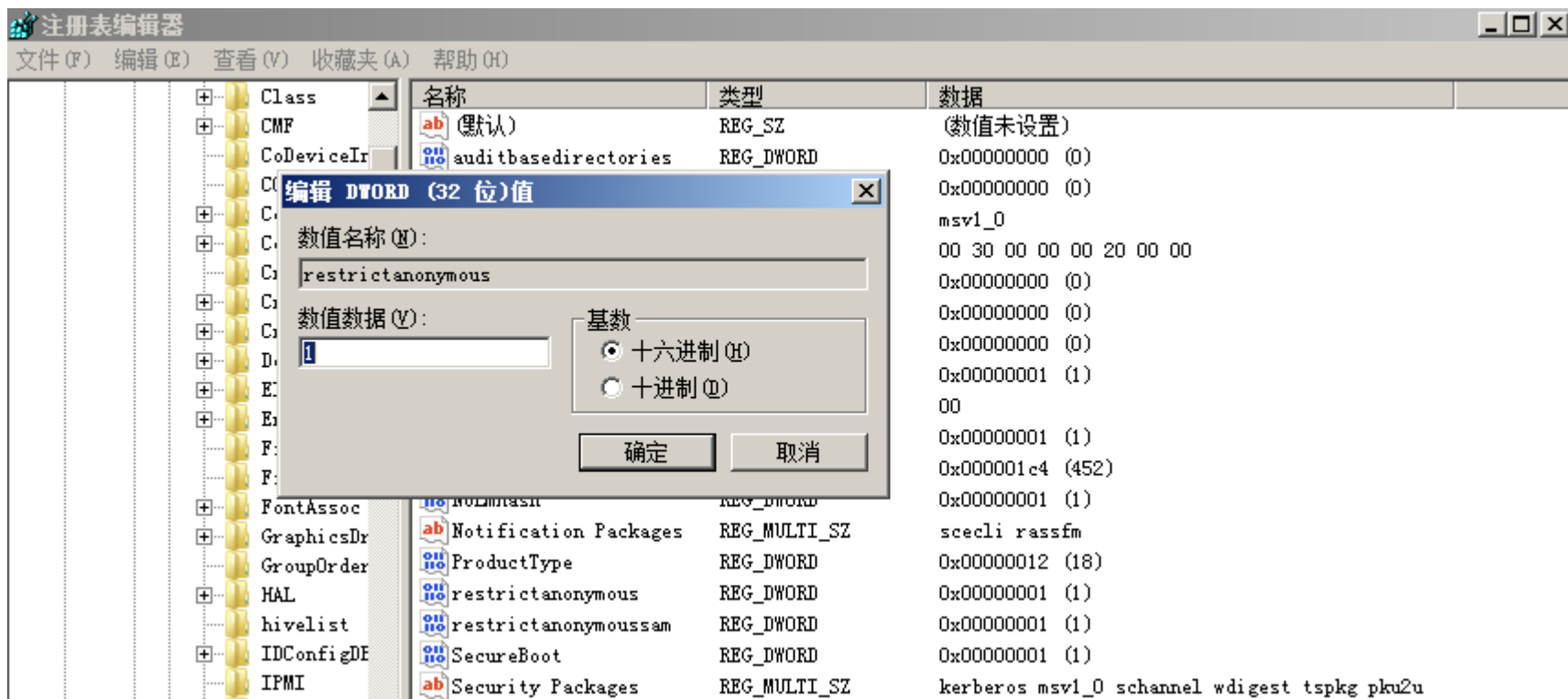
禁止空链接

删除IPC共享

禁用IPC连接，编辑注册表

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\restrictanonymous值为1

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa" /v  
restrictanonymous /d 0 /f
```



删除系统默认共享

删除服务器上的管理员共享

HKLM\System\CurrentControlSet\

Services\LanmanServer\Parameters\AutoShareServer参数为0

使用net share命令查看默认共享

```
C:\Documents and Settings\Administrator>net share
```

共享名	资源	注释
ADMIN\$	C:\WINDOWS	远程管理
C\$	C:\	默认共享
IPC\$		远程 IPC

命令成功完成。

使用net share <共享名> /del 删除默认共享

```
C:\Documents and Settings\Administrator>net share ADMIN$ /del
ADMIN$ 已经删除。

C:\Documents and Settings\Administrator>net share C$ /del
C$ 已经删除。
```

修改默认3389远程端口

修改注册表

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal
Server\Wds\rdpwd\Tds\tcp\PortNumber

它默认值是3389，这样我们可以修改成自己的想要的端口号，修改的时候要选十进制。

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal  
Server\Wds\rdpwd\Tds\tcp" /v PortNumber /d 4445 /f
```



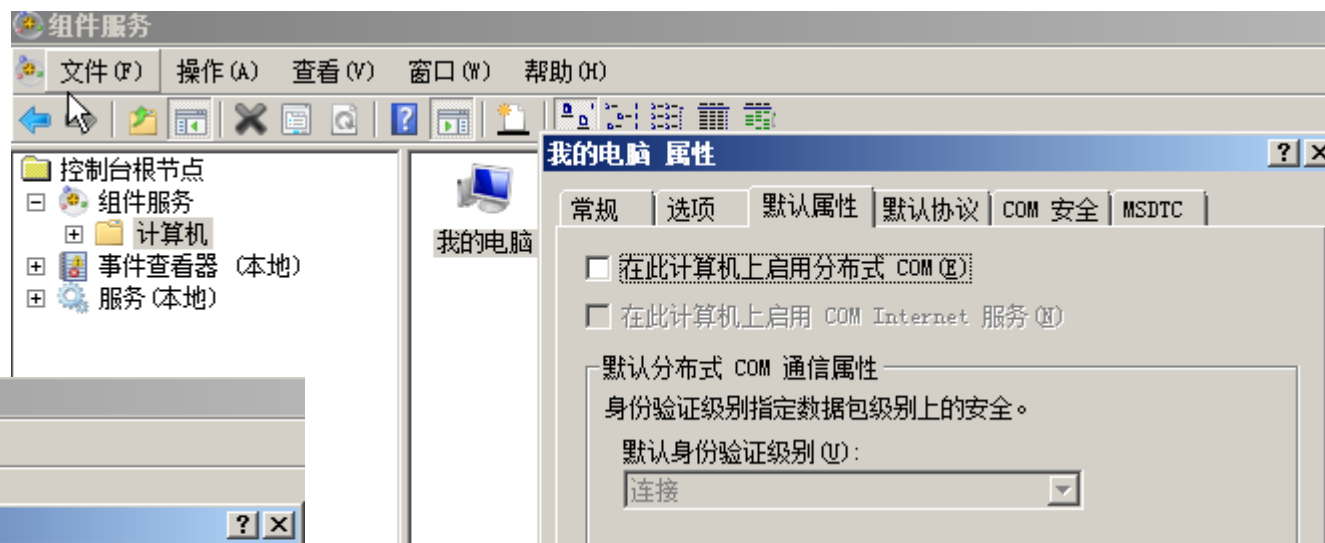
关闭135.139.445隐患端口

关闭135端口

”开始“--“运行”，输入”dcomcnfg”，单击“确定”，打开组件服务

右键我的电脑，单击”属性”，在默认属性中去掉”在此计算机上启用分布式COM”前的勾

选择”默认协议”选项卡，选中“面向连接的TCP/IP”，单击”确定”按钮，设置完成，重新启动后即可关闭135端口



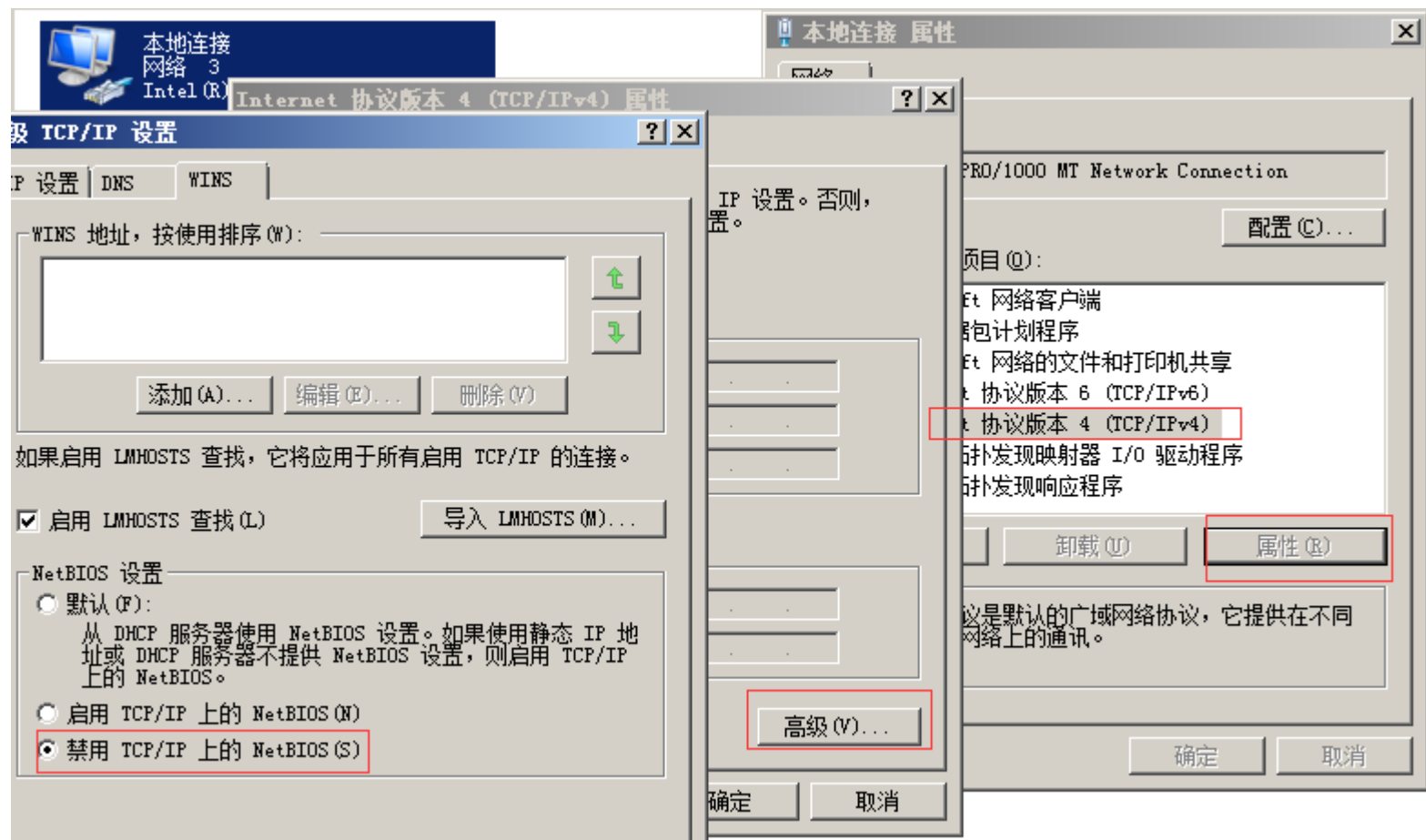
关闭135.139.445隐患端口

关闭139端口

右键我的“网上邻居”，单击“属性”，再打开本地连接的“属性”

选中Internet协议(TCP/IP),常规选项卡-高级

设置WINS选项卡“禁用TCP/IP上的NETBIOS”



关闭135.139.445隐患端口

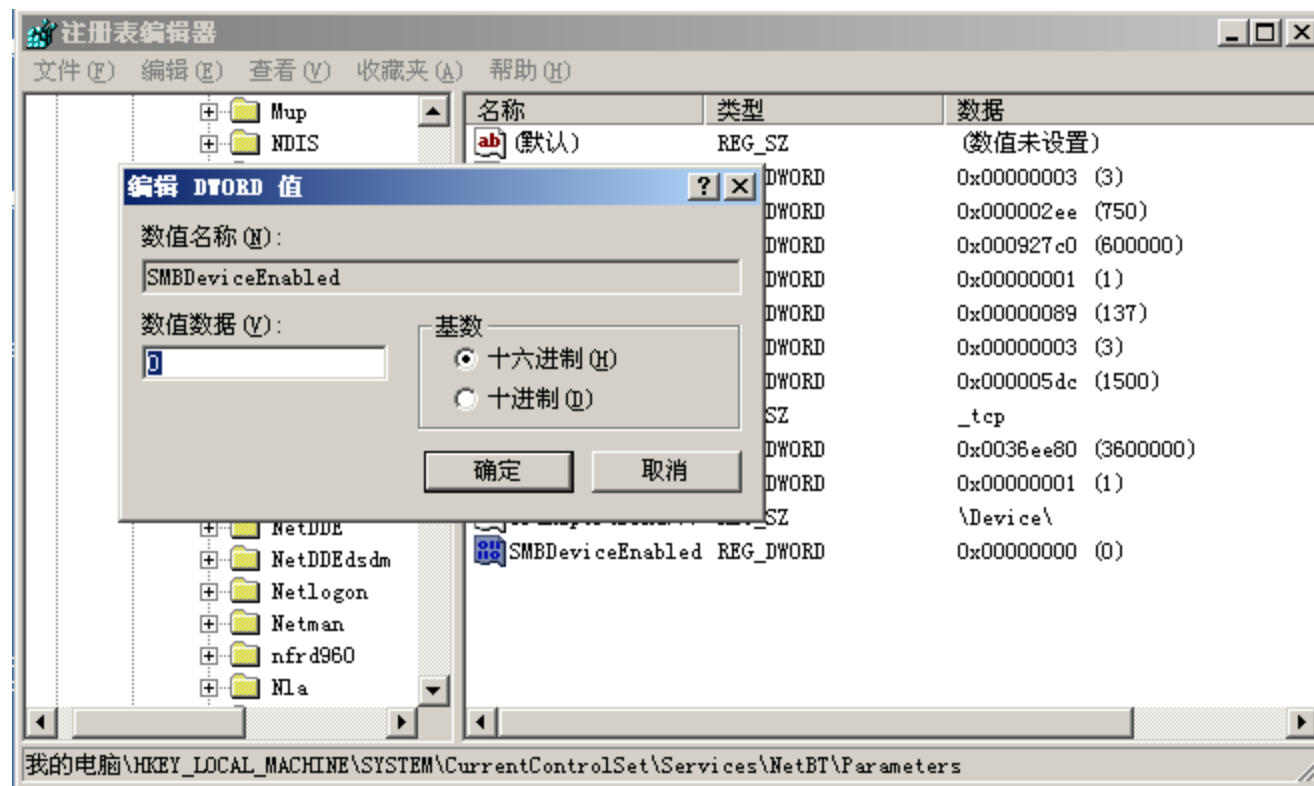
关闭445端口

修改注册表，添加一个键值

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters在右面的窗口

新建一个SMBDeviceEnabled 为REG_DWORD类型键值为 0。

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\NetBT" /v  
SMBDeviceEnabled /t REG_DWORD /d 0 /f
```



让配置立即生效

- 一、修改完后立即生效
- 二、重启explorer.exe进程就可以让修改注册表生效
- 三、重启计算机

谢谢