@echo off

title= Windwos/index.html' target='\_blank'>Windows Security

echo.

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

echo. Common Security Configuration For Windows Server 2003

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

echo.

echo.

rem 删除不必要的文件

del /Q /F C:\WINDOWS\Web\printers\\*.\*

del /Q /F C:\WINDOWS\system32\inetsrv\iisadmpwd\\*.\*

rd C:\WINDOWS\Web\printers\ /S /Q

rd C:\WINDOWS\help\iishelp\ /S /Q

rem 设置脚本宿主

cscript //h:cscript

rem 安装windows install服务

msiexec /regserver

regsvr32 msxml3.dll /s

rem 设置每个磁盘分区的权限

cd\

echo y | cacls C: /C /E /G administrators:F system:F

rem cacls /C D: /G administrators:F system:F

rem cacls /C E: /G administrators:F system:F

rem 设置关键目录的权限

echo y | cacls %SYSTEMROOT% /G administrators:F system:F users:C

echo y | cacls %SYSTEMROOT%\Temp /G administrators:F system:F everyone:F

rem 清除关键目录everyone权限

echo y | cacls C:\Docume~1 /E /R everyone

echo y | cacls C:\Docume~1\alluse~1 /E /R everyone

echo y | cacls C:\Docume~1\alluse~1\applic~1 /E /R everyone

echo y | cacls C:\Docume~1\defaul~1 /E /R everyone

echo y | cacls %SYSTEMROOT%\Installer /E /R everyone

echo y | cacls %SYSTEMROOT%\PCHealth /E /R everyone

for %%i in (

%SYSTEMROOT%\regedit.exe

%SYSTEMROOT%\system32\net.exe

%SYSTEMROOT%\system32\telnet.exe

%SYSTEMROOT%\system32\cmd.exe

%SYSTEMROOT%\system32\tftp.exe

%SYSTEMROOT%\system32\netstat.exe

%SYSTEMROOT%\system32\attrib.exe

%SYSTEMROOT%\system32\cacls.exe

%SYSTEMROOT%\system32\format.com

%SYSTEMROOT%\system32\regsvr32.exe

%SYSTEMROOT%\system32\xcopy.exe

%SYSTEMROOT%\system32\wscript.exe

%SYSTEMROOT%\system32\cscript.exe

%SYSTEMROOT%\system32\ftp.exe

%SYSTEMROOT%\system32\arp.exe

%SYSTEMROOT%\system32\edlin.exe

%SYSTEMROOT%\system32\ping.exe

%SYSTEMROOT%\system32\route.exe

%SYSTEMROOT%\system32\finger.exe

%SYSTEMROOT%\system32\posix.exe

%SYSTEMROOT%\system32\atsvc.exe

%SYSTEMROOT%\system32\qbasic.exe

%SYSTEMROOT%\system32\runonce.exe

%SYSTEMROOT%\system32\syskey.exe

%SYSTEMROOT%\system32\command.com

%SYSTEMROOT%\system32\edit.com

%SYSTEMROOT%\system32\tree.com

%SYSTEMROOT%\system32\at.exe

%SYSTEMROOT%\system32\find.exe

%SYSTEMROOT%\system32\fc.exe

%SYSTEMROOT%\system32\nbtstat.exe

%SYSTEMROOT%\system32\netsh.exe

%SYSTEMROOT%\system32\notepad.exe

%SYSTEMROOT%\system32\tasklist.exe

%SYSTEMROOT%\system32\taskkill.exe

%SYSTEMROOT%\system32\dllcache\regedit.exe

%SYSTEMROOT%\system32\dllcache\net.exe

%SYSTEMROOT%\system32\dllcache\telnet.exe

%SYSTEMROOT%\system32\dllcache\cmd.exe

%SYSTEMROOT%\system32\dllcache\tftp.exe

%SYSTEMROOT%\system32\dllcache\netstat.exe

%SYSTEMROOT%\system32\dllcache\attrib.exe

%SYSTEMROOT%\system32\dllcache\cacls.exe

%SYSTEMROOT%\system32\dllcache\format.com

%SYSTEMROOT%\system32\dllcache\regsvr32.exe

%SYSTEMROOT%\system32\dllcache\xcopy.exe

%SYSTEMROOT%\system32\dllcache\wscript.exe

%SYSTEMROOT%\system32\dllcache\cscript.exe

%SYSTEMROOT%\system32\dllcache\ftp.exe

%SYSTEMROOT%\system32\dllcache\arp.exe

%SYSTEMROOT%\system32\dllcache\edlin.exe

%SYSTEMROOT%\system32\dllcache\ping.exe

%SYSTEMROOT%\system32\dllcache\route.exe

%SYSTEMROOT%\system32\dllcache\finger.exe

%SYSTEMROOT%\system32\dllcache\posix.exe

%SYSTEMROOT%\system32\dllcache\atsvc.exe

%SYSTEMROOT%\system32\dllcache\qbasic.exe

%SYSTEMROOT%\system32\dllcache\runonce.exe

%SYSTEMROOT%\system32\dllcache\syskey.exe

%SYSTEMROOT%\system32\dllcache\command.com

%SYSTEMROOT%\system32\dllcache\edit.com

%SYSTEMROOT%\system32\dllcache\tree.com

%SYSTEMROOT%\system32\dllcache\at.exe

%SYSTEMROOT%\system32\dllcache\find.exe

%SYSTEMROOT%\system32\dllcache\fc.exe

%SYSTEMROOT%\system32\dllcache\nbtstat.exe

%SYSTEMROOT%\system32\dllcache\netsh.exe

%SYSTEMROOT%\system32\dllcache\notepad.exe

%SYSTEMROOT%\system32\dllcache\tasklist.exe

%SYSTEMROOT%\system32\dllcache\taskkill.exe

) do (

if exist "%%i" (

echo y | cacls %%i /G administrators:F system:F

)

)

rem 保存当前服务启动状态

net start > %systemroot%\security\services.txt

rem 设置自动启动的服务

sc config wuauserv start= auto

sc config PolicyAgent start= auto

sc config schedule start= auto

sc config NSClientpp start= auto

net start PolicyAgent

net start wuauserv

net start schedule

net start NSClientpp

net start winmgmt

rem 设置手动启动的服务

sc config winmgmt start= demand

sc config msdtc start= demand

rem 设置禁止启动的服务,停止启动的服务

for %%i in (

sharedaccess

helpsvc

Spooler

audiosrv

wmdmpmsn

Alerter

alg

TrkWks

seclogon

ShellHWDetection

lanmanserver

dmserver

Dhcp

lanmanworkstation

LmHosts

WZCSVC

RemoteRegistry

AeLookupSrv

Dnscache

ERSvc

Nla

SCardSvr

W32Time

w3svc

IISADMIN

SMTPSVC

TapiSrv

WinRM

dfs

ntfrs

CiSvc

mnmsrvc

clipsrv

netdde

NetDDEdsdm

lmhosts

tlntsvr

ups

themes

HidServ

Tssdis

stisvc

WmiApSrv

awhost32

fax

Browser

) do (

sc config %%i start= disabled

net stop %%i

)

rem 设置每天3点自动重启

rem schtasks /create /ru system /sc daily /tn "restart" /st 03:00:00 /tr "shutdown -r -f -t 30"

rem 设置环境变量

rem reg add "HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment" /v JAVA\_HOME /t REG\_SZ /d C:\jdk /f

rem reg add "HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment" /v Path /t REG\_EXPAND\_SZ /d "%JAVA\_HOME%\bin;%SystemRoot%\system32;%SystemRoot%;%SystemRoot%\System32\Wbem;" /f

echo 开启远程桌面

reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t reg\_dword /d 0 /f

rem 修改远程桌面端口为9999

rem reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp" /v PortNumber /t reg\_dword /d 9999 /f

rem reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v PortNumber /t reg\_dword /d 9999 /f

echo 关闭CD-ROM自动运行

reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer" /v NoDriveTypeAutoRun /t reg\_dword /d 255 /f

echo 显示文件扩展名

reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced" /v HideFileExt /t reg\_dword /d 0 /f

echo 修改windows update为自动更新

reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update" /v AUOptions /t reg\_dword /d 1 /f

echo 华生医生设置为转储线程上下文

reg add HKLM\SOFTWARE\Microsoft\DrWatson /v AppendToLogFile /t reg\_dword /d 0 /f

reg add HKLM\SOFTWARE\Microsoft\DrWatson /v CreateCrashDump /t reg\_dword /d 0 /f

reg add HKLM\SOFTWARE\Microsoft\DrWatson /v WaveFile /t REG\_EXPAND\_SZ /d "" /f

echo 设置自动重新启动不发送管理警报

reg add HKLM\SYSTEM\ControlSet001\Control\CrashControl /v AutoReboot /t reg\_dword /d 1 /f

reg add HKLM\SYSTEM\ControlSet001\Control\CrashControl /v SendAlert /t reg\_dword /d 0 /f

echo 设置写入调试信息为无

reg add HKLM\SYSTEM\CurrentControlSet\Control\CrashControl /v CrashDumpEnabled /t reg\_dword /d 0 /f

echo 禁用错误报告

reg add HKLM\SOFTWARE\Microsoft\PCHealth\ErrorReporting /v DoReport /t reg\_dword /d 0 /f

reg add HKLM\SOFTWARE\Microsoft\PCHealth\ErrorReporting /v ShowUI /t reg\_dword /d 0 /f

echo 关机清理虚拟内存

reg add "HKLM\System\CurrentControlSet\Control\Session Manager\Memory Management" /v ClearPageFileAtShutdown /t reg\_dword /d 1 /f

echo 不显示上次登录用户名

reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System /v dontdisplaylastusername /t reg\_dword /d 1 /f

echo 关闭445端口

reg add HKLM\SYSTEM\CurrentControlSet\Services\NetBT\Parameters /v SMBDeviceEnabled /t reg\_dword /d 0 /f

echo 防止小规模ddos攻击

reg add HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters /v SynAttackProtect /t reg\_dword /d 1 /f

echo 禁止建立空连接

reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa /v restrictanonymous /t reg\_dword /d 1 /f

echo 禁止SAM 账户和共享的匿名枚举

reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa /v restrictanonymoussam /t reg\_dword /d 1 /f

echo 禁止系统自动管理共享

reg add HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters /v AutoShareWks /t reg\_dword /d 0 /f

echo 禁止系统自动共享

reg add HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters /v AutoShareServer /t reg\_dword /d 0 /f

rem 自动关闭无响应程序

rem reg add "HKCU\Control Panel\Desktop" /v AutoEndTasks /t reg\_sz /d 1 /f

echo 设置无法关闭程序等待时间

reg add "HKCU\Control Panel\Desktop" /v WaitToKillAppTimeout /t reg\_sz /d 100 /f

reg add "HKCU\Control Panel\Desktop" /v HungAppTimeout /t reg\_sz /d 500 /f

reg add HKLM\System\CurrentControlSet\Control /v WaitToKillServiceTimeout /t reg\_sz /d 100 /f

echo 不需要按ctrl+alt+del

reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system /v DisableCAD /t reg\_dword /d 1 /f

echo 把显示“关闭事件跟踪程序” 更改为已禁用

reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Reliability" /v ShutdownReasonOn /t reg\_dword /d 0 /f

echo 禁止自动更新后不断的提示重启

reg add HKLM\SOFTWARE\Policies\Microsoft\Windows\windowsUpdate /v RebootRelaunchTimeoutEnabled /t reg\_DWORD /d 1 /f

echo 禁止屏保

reg add "hkcu\Software\Policies\Microsoft\Windows\Control Panel\Desktop" /v ScreenSaveActive /t REG\_SZ /d 0 /f

echo 是否起用WSUS服务器

reg add HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU /v UseWUServer /t REG\_DWORD /d 1 /f

echo WSUS服务器设置

reg add HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate /v WUServer /t REG\_SZ /d http://61.135.177.110 /f

reg add HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate /v WUStatusServer /t REG\_SZ /d http://61.135.177.110 /f

echo 重新计划自动更新计划后的等待时间

reg add HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU /v RescheduleWaitTime /t REG\_DWORD /d 10 /f

echo 自动更新安装后是否重新启动

reg add HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU /v NoAutoRebootWithLoggedOnUsers /t REG\_DWORD /d 0 /f

echo 是否启用自动更新

reg add HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU /v NoAutoUpdate /t REG\_DWORD /d 0 /f

echo 配置自动更新

reg add HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU /v AUOptions /t REG\_DWORD /d 4 /f

echo 计划安装日期

reg add HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU /v ScheduledInstallDay /t REG\_DWORD /d 0 /f

echo 计划安装时间

reg add HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU /v ScheduledInstallTime /t REG\_DWORD /d 3 /f

rem 重命名管理员以及来宾帐户名称

rem wmic useraccount where name='Administrator' call Rename admin

echo 禁用帐户

net user SQLDebugger /active:no

net user TsInternetUser /active:no

echo 设置当前目录为桌面

if exist %USERPROFILE%\桌面\ (

cd/D %USERPROFILE%\桌面\

) else (

cd/D %USERPROFILE%\desktop\

)

echo 生成windows组策略安全设置

if exist secinit.inf del secinit.inf /f

echo [Unicode] >secinit.inf

echo. >>secinit.inf

echo [Event Audit] >>secinit.inf

echo AuditSystemEvents = 3 >>secinit.inf

echo AuditLogonEvents = 3 >>secinit.inf

echo AuditObjectAccess = 2 >>secinit.inf

echo AuditPrivilegeUse = 2 >>secinit.inf

echo AuditPolicyChange = 3 >>secinit.inf

echo AuditAccountManage = 3 >>secinit.inf

echo AuditProcessTracking = 0 >>secinit.inf

echo AuditDSAccess = 2 >>secinit.inf

echo AuditAccountLogon = 3 >>secinit.inf

echo [System Access] >>secinit.inf

echo MinimumPasswordAge = 0 >>secinit.inf

echo MaximumPasswordAge = 42 >>secinit.inf

echo MinimumPasswordLength = 12 >>secinit.inf

echo PasswordComplexity = 1 >>secinit.inf

echo PasswordHistorySize = 0 >>secinit.inf

echo LockoutBadCount = 5 >>secinit.inf

echo ResetLockoutCount = 20 >>secinit.inf

echo LockoutDuration = 20 >>secinit.inf

echo RequireLogonToChangePassword = 0 >>secinit.inf

echo ForceLogoffWhenHourExpire = 0 >>secinit.inf

echo ClearTextPassword = 0 >>secinit.inf

echo LSAAnonymousNameLookup = 0 >>secinit.inf

echo EnableAdminAccount = 1 >>secinit.inf

echo EnableGuestAccount = 0 >>secinit.inf

echo [System Log] >> secinit.inf

echo MaximumLogSize = 16384 >> secinit.inf

echo AuditLogRetentionPeriod = 1 >> secinit.inf

echo RetentionDays = 30 >> secinit.inf

echo [Security Log] >> secinit.inf

echo MaximumLogSize = 16384 >> secinit.inf

echo AuditLogRetentionPeriod = 1 >> secinit.inf

echo RetentionDays = 30 >> secinit.inf

echo [Application Log] >> secinit.inf

echo MaximumLogSize = 16384 >> secinit.inf

echo AuditLogRetentionPeriod = 1 >> secinit.inf

echo RetentionDays = 30 >> secinit.inf

echo [File Security] >> secinit.inf

echo "c:\boot.ini",2,"D:P(A;;GXGR;;;PU)(A;;GA;;;BA)(A;;GA;;;SY)" >> secinit.inf

echo "c:\ntdetect.com",2,"D:P(A;;GXGR;;;PU)(A;;GA;;;BA)(A;;GA;;;SY)" >> secinit.inf

echo "c:\ntldr",2,"D:P(A;;GXGR;;;PU)(A;;GA;;;BA)(A;;GA;;;SY)" >> secinit.inf

echo "c:\ntbootdd.sys",2,"D:P(A;;GXGR;;;PU)(A;;GA;;;BA)(A;;GA;;;SY)" >> secinit.inf

echo "c:\autoexec.bat",2,"D:P(A;;GXGR;;;BU)(A;;GXGR;;;PU)(A;;GA;;;BA)(A;;GA;;;SY)" >> secinit.inf

echo "c:\config.sys",2,"D:P(A;;GXGR;;;BU)(A;;GXGR;;;PU)(A;;GA;;;BA)(A;;GA;;;SY)" >> secinit.inf

echo "%ProgramFiles%",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)" >> secinit.inf

echo "%SystemRoot%",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)(A;;GXGR;;;WD)" >> secinit.inf

echo "%SystemRoot%\explorer.exe",2,"D:(A;;GXGR;;;WD)" >> secinit.inf

echo "%SystemRoot%\CSC",1,"D:AR" >> secinit.inf

echo "%SystemRoot%\debug",1,"D:AR" >> secinit.inf

echo "%SystemRoot%\Offline Pages",1,"D:AR" >> secinit.inf

echo "%SystemRoot%\Profiles",1,"D:AR" >> secinit.inf

echo "%SystemRoot%\Registration",1,"D:AR" >> secinit.inf

echo "%SystemRoot%\repair",2,"D:P(A;CI;GXGR;;;BU)(A;CI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)" >> secinit.inf

echo "%SystemRoot%\Tasks",1,"D:AR" >> secinit.inf

echo "%SystemRoot%\Temp",2,"D:P(A;CI;0x100026;;;BU)(A;CI;0x100026;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)" >> secinit.inf

echo "%SystemRoot%\addins",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)" >> secinit.inf

echo "%SystemRoot%\Connection Wizard",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)" >> secinit.inf

echo "%SystemRoot%\Driver Cache",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)" >> secinit.inf

echo "%SystemRoot%\java",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)" >> secinit.inf

echo "%SystemRoot%\msagent",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)" >> secinit.inf

echo "%SystemRoot%\security",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)" >> secinit.inf

echo "%SystemRoot%\speech",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)" >> secinit.inf

echo "%SystemRoot%\twain\_32",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)" >> secinit.inf

echo "%SystemRoot%\Web",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)" >> secinit.inf

echo [Registry Values] >>secinit.inf

echo MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName=4,1 >> secinit.inf

echo MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,1 >> secinit.inf

echo [Privilege Rights] >>secinit.inf

echo SeNetworkLogonRight = Administrators >> secinit.inf

echo SeShutdownPrivilege = Administrators >> secinit.inf

echo SeRemoteShutdownPrivilege = Administrators >> secinit.inf

echo SeRemoteInteractiveLogonRight = Administrators >> secinit.inf

echo Seinteractivelogonright = Administrators >> secinit.inf

echo [Version] >>secinit.inf

echo signature="$CHICAGO$" >>secinit.inf

echo Revision=1 >>secinit.inf

cls

echo 运行安全设置

move /y secinit.inf %systemroot%\security\templates\secinit.inf

echo y|secedit /configure /cfg %systemroot%\security\templates\secinit.inf /db %systemroot%\security\database\secinit.db /overwrite /log %systemroot%\security\logs\secinit.log

regsvr32 /s scecli.dll

echo 关闭默认共享

net share c$ /del

net share d$ /del

net share e$ /del

net share ipc$ /del

net share admin$ /del

del secinit.inf /f