Securing IIS/Windows 2000 against Internet Vandals Whitepaper

Written by Dave Ellis

dellis@nightwatchnss.com

NightWatch Network & Security Solutions

http://www.nightwatchnss.com

.1 Objective 2

.2 Installation 3

System Installation 3

Recommended Patches 5

Creating Emergency Repair Disk 6

Account settings : 7

Applay Security Policy: 7

Recommended settings for security policy 9

Protecting Files and Directories 17

.3 IIS Application Security 21

General Services 21

IIS Configuration 22

1. Objective

The purpose of this document is to provide a technical security checklist which will be used during the installation of IIS version 5 with on a Win 2000 platform in a secure mode.

While writing this document, we considered that the server will be used as an Internet server and not an internal web server.

The checklist deals with the installation of the Win 2000 and IIS ver 5. It is important to emphasize that the security level is also affected from the web application that will be installed over the IIS server. Therefore, the application level security has to be defined during the development.

2. Installation

System Installation

Installation Order:

- Windows 2000 Server Installation
- System configuration
- Install Internet Information Server 5.0
- Install Windows 2000 latest Service Pack
- Apply Hot Fixes as listed in Hot Fix List
- Creating Recovery Disk
- Apply Security Policy
- Internet Information Server 5.0 Specific Configuration

System Configuration Pre requirements:

- Machine is a not a Domain Controller
- If machine is joined to a domain, it should be in it's own OU
- Machine is a dedicated web-server
- Machine has the Windows 2000 clean-install defaults
- No modifications have been made to ACLs, User Rights etc

ARMORING WINDOWS 2000 SECURE CHECKLIST

Server Name: _____

Before you start doing anything, you must create an Emergency Repair disk!

System Configuration Information

Requested Installation Information	
Network adapter card name and model number	
Graphic adapter name and model number	
Number of partitions on the hard drive (recommend two partitions: one partition for the operating system, one partition for data and applications)	
IP address of the computer	
IP address of the Domain Name Service (DNS/DDNS) server	
Active Directory Installed	
IP address of DHCP server (if the DHCP service is used instead of a static IP address for the computer)	
IP addresses of the primary and secondary WINS servers	
Subnet mask	
IP address of the default gateway	
Name of the domain the workstations will join or servers will control	
Licensing method (per server or per seat)	
Computer name, up to 15 characters in length	

Disk Partitioning:

- *All partitions should be formated in NTFS. FAT Partitions should be converted in the following manner:*

  Run: Convert [drive:] /fs:ntfs

Encrypt the Sam Database:

- use the syskey option to encrypt the sam in 128 bit.

  Run: winnt/system32/syskey.exe

Recommended Patches

- Install Windows 2000 Service Pack 3
  Can be Downloaded from :

  www.microsoft.com/windows2000/downloads/recommended/sp3/ default.asp

- All Following Patches are System and Security Fixes, all post Service Pack.
  Can be Downloaded from:

  www.microsoft.com/windows2000/downloads/default.asp

  IISLockDownTool
  All the latest Cumulative Patchs
  The Latest IE
  Latest Antivirus Signature File.

Recommended Patches:

hfnetchk.exe Util which will check the machine for the latest Patchs. Run hfnetchk then run a program called update expert which seamlessly installs all security patches from microsofts web site.

- Many of the Windows 2000 settings are configurable through the provided security template (hisecweb,inf); there is no need to manually configure Registry settings.
- Some of the less-secure default settings in Microsoft Windows NT 4 and Internet Information Server 4 are disabled by default in Windows 2000 and IIS 5.

Download this template and import it to c:\winnt\security\ template.

Hisecweb.inf can be downloaded from:
http://download.microsoft.com/download/win2000srv/SCM/1.0/NT5/EN-US/hisecweb.exe

Then open mmc | security configuration and Analysis | Analyze the computer .

- ***I recommend installing the "systemscanner" (ISS) from the win2k reskit for last Security Checks.***

Creating Emergency Repair Disk

- Recovery disk has to be created before starting the hardening procedure.

  Start-> programs ->accessories -> system tools -> backup

Registry Changes

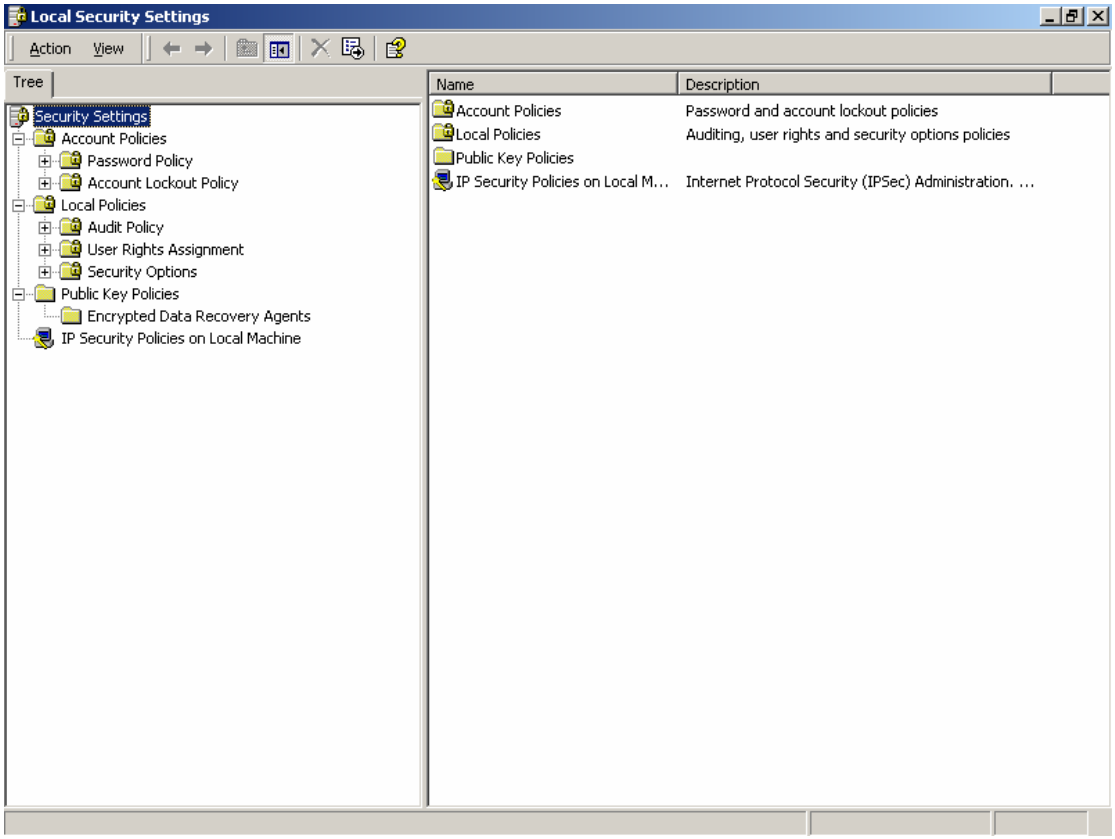
At the bottom of this document is a script that you can alter to your liking. Just copy and paste it into notepad then rename it with a .reg extension. When you run, it will ask you if you want to import the following changes in the registry, Say Yes.

Account settings :

1. Rename administrator built in account and define at least 9 charecters password . Use strong passwords – alphanumeric and symbols. DON'T USE DICTIONARY WORDS. Remove description
2. Create a new account with no permissions and name it as administrator .
3. Disable guest account and remove description .
4. Check all high privileged groups for unnecessary users .
5. Make sure that all users have a unique accounts .

Apply Security Policy:

- Apply the security settings using Security policy tool.


Local Security Settings
Action
View
Tree
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Public Key Policies
Encrypted Data Recovery Agents
IP Security Policies on Local Machine
Name
Description
Account Policies
Password and account lockout policies
Local Policies
Auditing, user rights and security options policies
Public Key Policies
IP Security Policies on Local M...
Internet Protocol Security (IPSec) Administration. ...

Recommended settings for security policy

Changes are made in the following:

Account policies:

- Password Policy
- Account LockOut Policy

Local Policies:

- Audit policy
- User Rights Assignment
- Security Options

Password Policy:

Policy	Changed To:
Enforce password history	passwords remembered 10
Maximum password age	90 days
Minimum password age	1 day
Minimum password length	6 characters[1]
Passwords must meet complexity requirements	Enabled[2]

[1] In order to meet the organization security common criteria.
[2] To be defined by Sec. Officer if this parameter is agreed (complexity).

Account lockout policy:

Policy	Change To:
Account lockout duration	45 minutes
Account lockout threshold	5 invalid[3] logon attempts
Reset account lockout counter after	30 minutes

Local Policies:

Audit Policies:

Audit Policy	Change To
Audit account logon events	Failure
Audit account management	Success, Failure
Audit directory service access	Failure
Audit logon events	Failure
Audit object access	Failure
Audit policy change	Success, Failure
Audit privilege use	Failure
Audit process tracking	Failure
Audit system events	Failure

[3] TBD – the number may be increase to 10 invalid logons.

User rights assignment:

User right	Changed To:
Access this computer from the network	**Authenticated Users** Administrators I_user
Act as part of the operating system	none
Add workstations to domain	Administrators
Back up files and directories	Administrators Backup operators Server operators
Bypass traverse checking	Administrators I_user
Change the system time	Administrators Server operators
Create a pagefile	Administrators
Create a token object	None
Create permanent shared objects	None
Debug programs	Administrators
Deny access to this computer from the network	Not defined
Deny logon as a batch job	Not defined
Deny logon as a service	Not defined
Deny logon locally	Not defined
Enable computer and user accounts to be trusted for delegation	Not defined

User right	Changed To:
Force shutdown from a remote system	Administrators Server operators
Generate security audits	Administrators
Increase quotas	Administrators
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	none
Log on as a batch job	none
Log on as a service	none
Log on locally	Administrators Backup operators Server operators Print operators
Manage auditing and security log	Administrators
Modify firmware environment values	Administrators
Profile single process	Administrators
Profile system performance	Administrators
Remove computer from docking station	Administrators
Replace a process level token	none
Restore files and directories	Administrators Backup operators Server operators
Shut down the system	Administrators Server operators
Synchronize directory service data	Administrators
Take ownership of files or other objects	Administrators

Security Options:

Policy	**Change To:**
Additional restrictions for anonymous connections	No access without explicit anonymous permissions
Allow system to be shut down without having to log on	Disabled
Allowed to eject removable NTFS media	Administrators
Amount of idle time required before disconnecting session	15 minutes
Audit the access of global system objects	Enabled
Audit use of Backup and Restore privilege	Enabled
Automatically log off users when logon time expires (local)	Enabled
Clear virtual memory pagefile when system shuts down	Enabled
Digitally sign client communication (always)	Disabled
Digitally sign client communication (when Possible)	Enabled
Digitally sign server communication (always)	Disabled
Digitally sign server communication (when possible)	Disabled
Disable CTRL+ALT+DEL requirement for logon	Disabled
Do not display last user name in logon screen	Enabled

Policy	**Change To:**
This Message text for users attempting to log on	Add your own text using the MMC Security Templates tool[4]
Message title for users attempting to log on	Attention!!!
Number of previous logons to cache (in case domain controller is not availabl)	0 logons
Prevent system maintenance of computer account password	Disabled
Prevent users from installing printer drivers	Enabled
Prompt user to change password before expiration	14 days
Recovery Console: Allow automatic administrative logon	Disabled
Recovery Console: Allow floppy copy and access to all drives and all folders	Disabled
Rename administrator account	Not defined
Rename guest account	Not defined
Restrict CD-ROM access to locally logged-on user only	Enabled
Restrict floppy access to locally logged-on user only	Enabled

[4] Legal Notice that should be defined by . Suggested:"This is a private network. Any unauthorized logon is prohibited. We shall prosecute

Policy	**Change To:**
Secure channel: Digitally encrypt or sign secure channel data (always)	Disabled
Secure channel: Digitally encrypt secure channel data (when possible)	Enabled
Secure channel: Digitally sign secure channel data (when possible)	Enabled
Secure channel: Require strong (Windows 2000 or later) session key	Disabled
Send unencrypted password to connect to third-party SMB servers	Disabled
Shut down system immediately if unable to log security audits	Disabled
Smart card removal behavior	No action
Strengthen default permissions of global system objects (e.g. Symbolic Links)	Enabled
Unsigned driver installation behavior	Do not allow installation
Unsigned non-driver installation behavior	Silently succeed

Install The IIS Lockdown Tool and Pick the appropriate template that suits your web page!!!

Disable all unnecessary services

Protecting Files and Directories

Among the files and directories to be protected are those that make up the operating system software itself. The standard set of permissions on system

files and directories provide a reasonable degree of security without interfering with the computer's usability. For high-level security installations, however, you might want to additionally set directory permissions to all subdirectories and existing files, as shown in the following list:
The caveat here of course is that these permissions should be applied right after Win 2000 install to reduce potential conflicts.

Directory	Permissions

All partitions	Administrators: Full Control CREATOR OWNER: Full Control Authenticated users :list SYSTEM: Full Control
C:\winnt\system32 Not including subdirectories , only existing files .	Administrators, CREATOR OWNER: Full Control AUTHENTICATED USERS: List SYSTEM: Full Control I_user - RX

Special file permissions for IIS

Permissions that have to be granted to I_user are listed below :

C:/Winnt/system32 define Only for this directory	change
C:/Winnt/system32/inetsrv	RX
C:/inetpub	RX

Disable or Remove All Sample Applications

Samples are just that, samples; they are not installed by default and should never be installed on a production server. Note that some samples install so that they can be accessed only from http://localhost, or 127.0.0.1; however, they should still be removed.

Sample **Virtual Directory** **Location**

IIS Samples	\IISSamples	c:\inetpub\iissamples
IIS Documentation	\IISHelp	c:\winnt\help\iishelp
Data Access	\MSADC	c:\program files\common files\system\msadc

Sample files included with Internet Information Server 5.

Remove the IISADMPWD Virtual Directory

This directory allows you to reset Windows NT and Windows 2000 passwords. It's designed primarily for intranet scenarios and is not installed as part of IIS 5, but it is not removed when an IIS 4 server is upgraded to IIS 5. It should be removed if you don't use an intranet or if you connect the server to the Web..

Remove Unused Script Mappings

IIS is preconfigured to support common filename extensions such as .asp and .shtm files. When IIS receives a request for a file of one of these types, the call is handled by a DLL. If you don't use some of these extensions or functionality, you should remove the mappings by following this procedure:

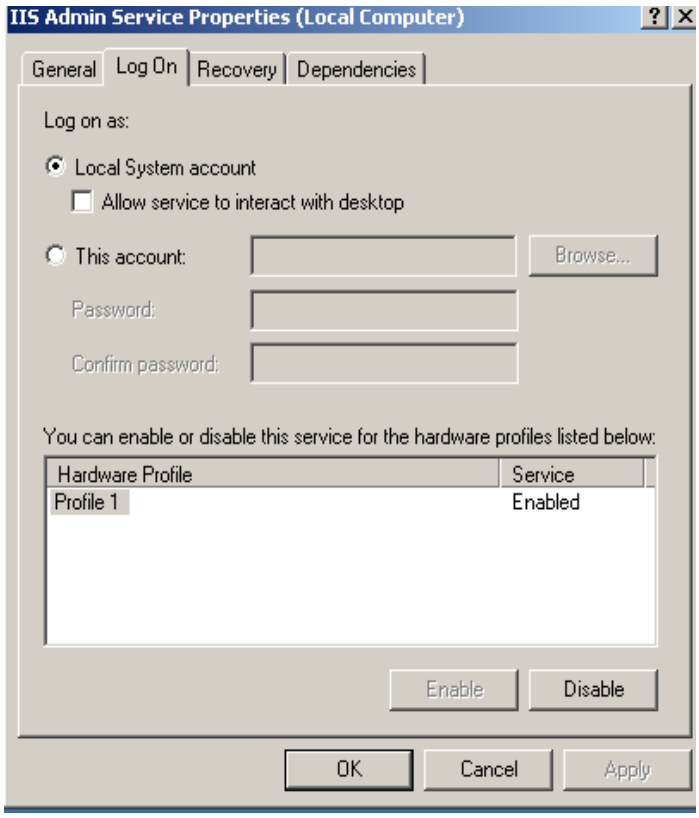
1. Open Internet Services Manager.
2. Right-click the Web server, and choose Properties from the context menu.
3. Master Properties
4. Select WWW Service | Edit | HomeDirectory | Configuration

Remove these references:

If you don't use...	Remove this entry:
Web-based password reset	.htr
Internet Database Connector (all IIS 5 Web sites should use ADO or similar technology)	.idc
Server-side Includes	.stm, .shtm and .shtml
Internet Printing	.printer
Index Server	.htw, .ida and .idq

3. IIS Application Security

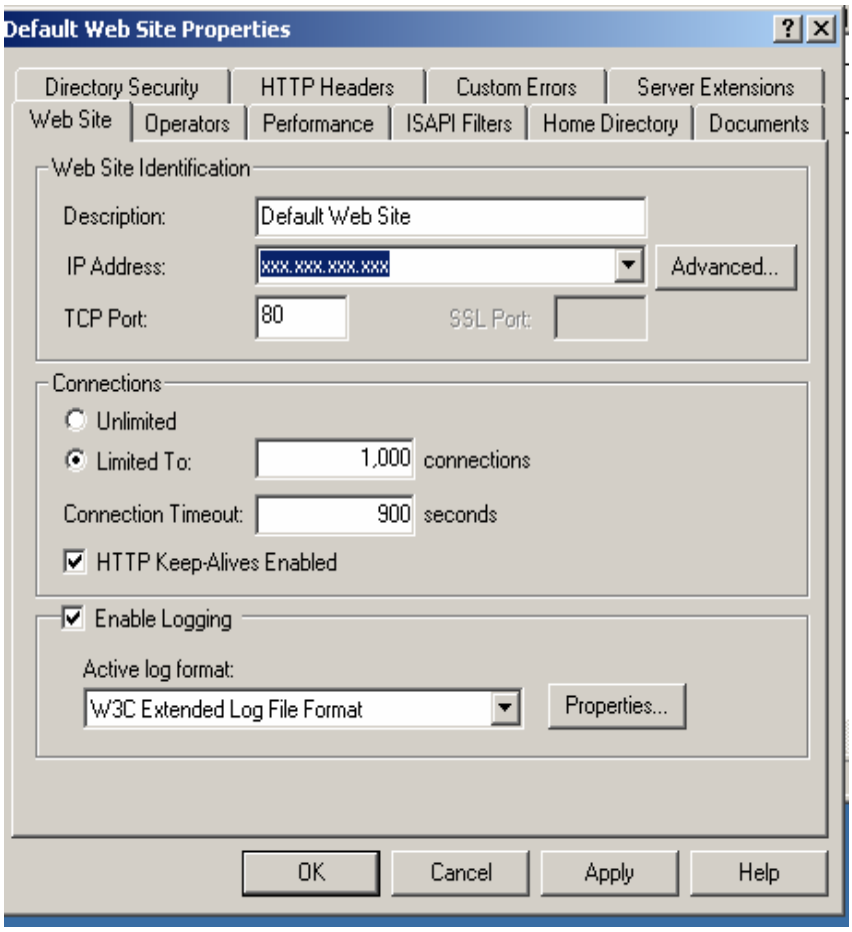
General Services



1. Every service needed (only http) of the iis application have to be start automaticly when the operating system is started .
2. The box : " allow services to interact with desktop " have to be unchecked .

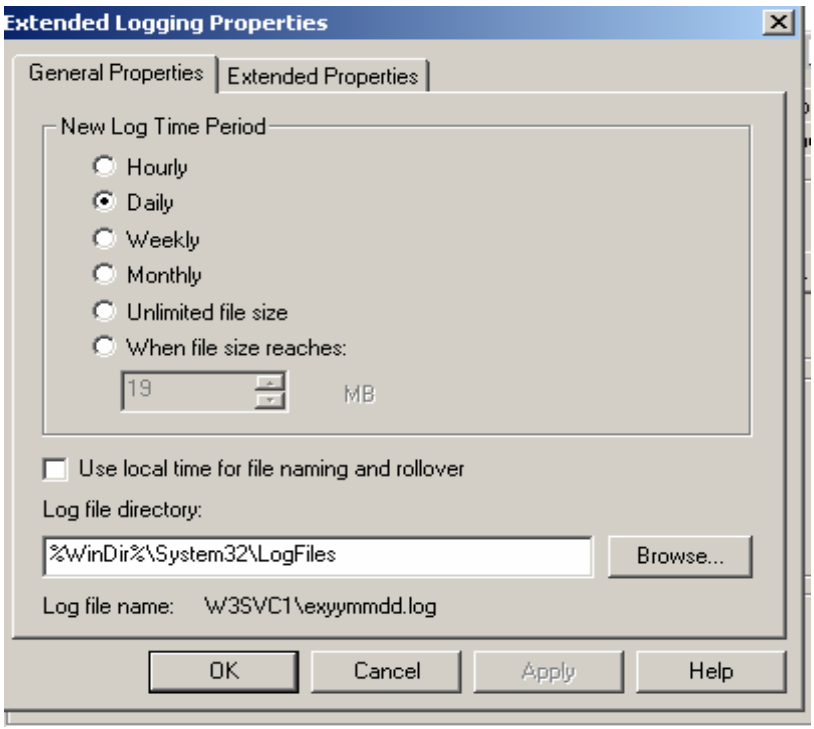
Default web site \ properties \ web site tab

Change Default website from the default directory



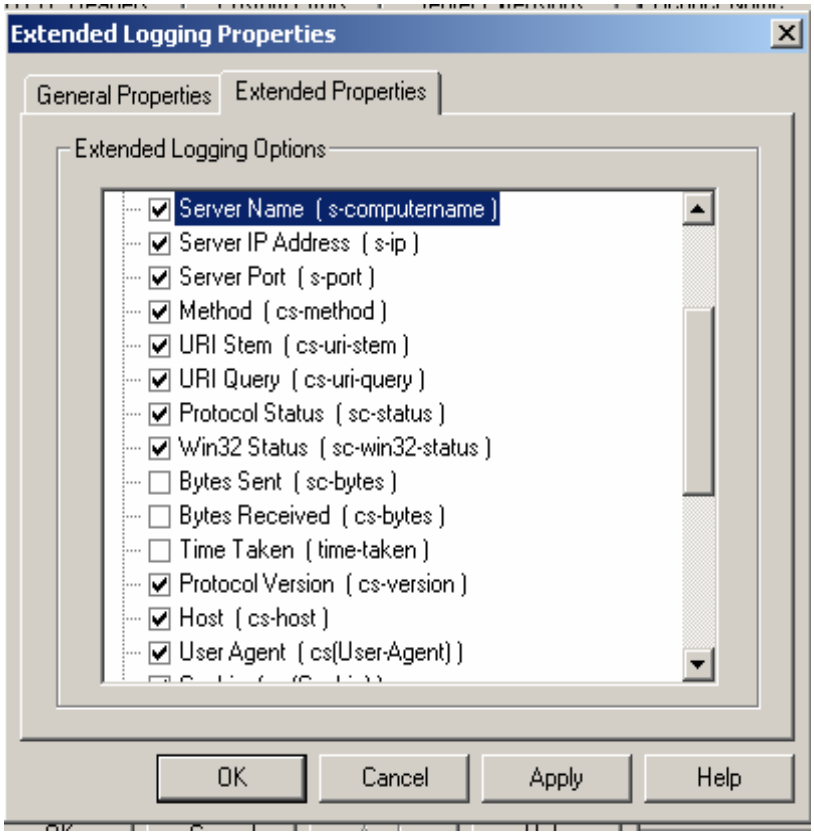
1. At the web site tab check the box : " enable logging "
2. Leave the active log format in his default definition (W3C extended log file format) .
3. At the IP address field define the ip address of the server which the iis is running on .
4. The connections to the iis server have to be limited . The limitation have to be defined with system administrator .

Default web site/properties/web site tab/properties/general properties tab



1. Define the new log time period to daily .
2. Locate the log files at NTFS partition and assign permissions only to administrator and system accounts .

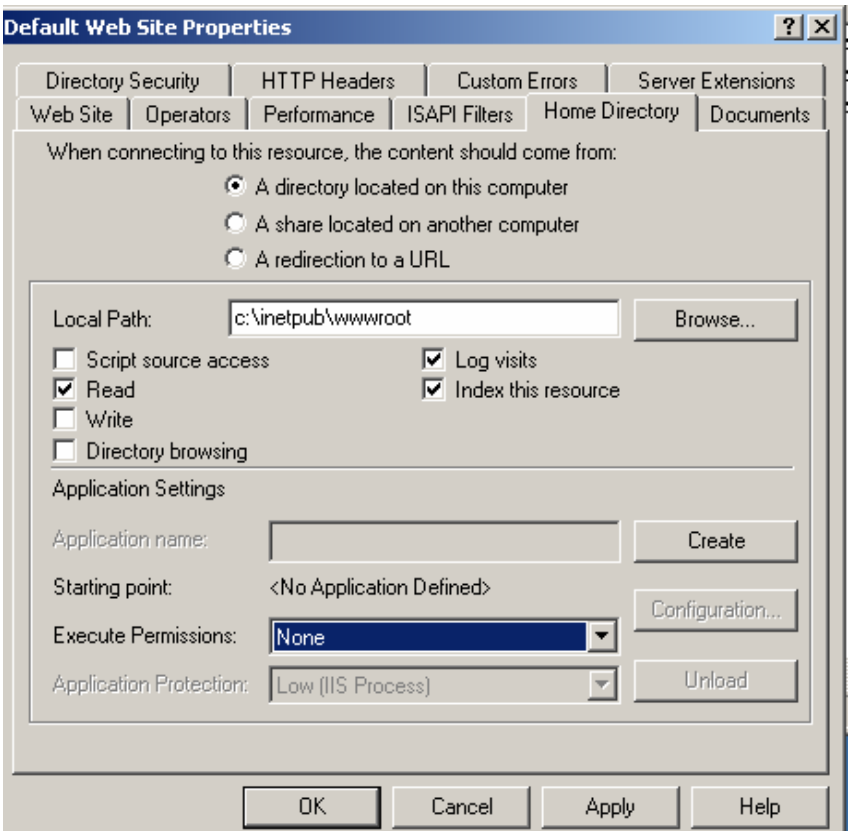
Default web site / properties / web site tab / properties / extended properties tab



In those tab, it should be defined all the events that will be written to log files. Not all events are defined by default .

Define all of the events besides bytes sent and bytes received. These log files would help to track users that tried to penetrate to web server .

Default web site / properties / home directory



Put all system files on the local server: “a directory located in this computer” should be marked.

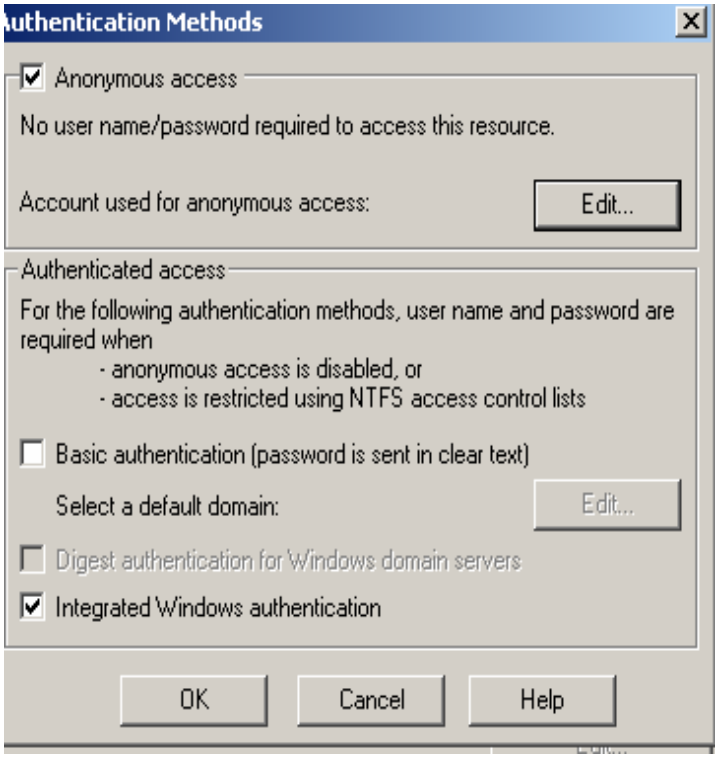
Rename the default directory (for example : rename Inetpub to Web).

Check the box “read” and “log visits” and Index this resource”.

If the web site is using scripts (asp , pl , Vbscripts) leave the application setting in default mode , if only part of the application is using scripts it’s recommended to remove the default application and script permissions .

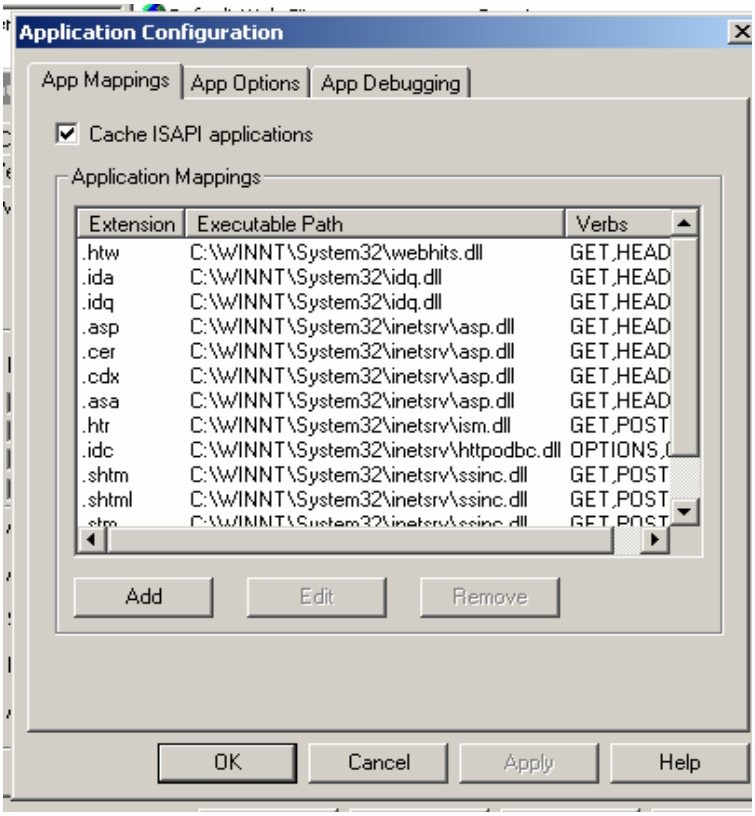
Check the box : “ run in separate memory space “ to define more reliable system .

Default web site / properties / web site tab / properties /directory security / authentication methods



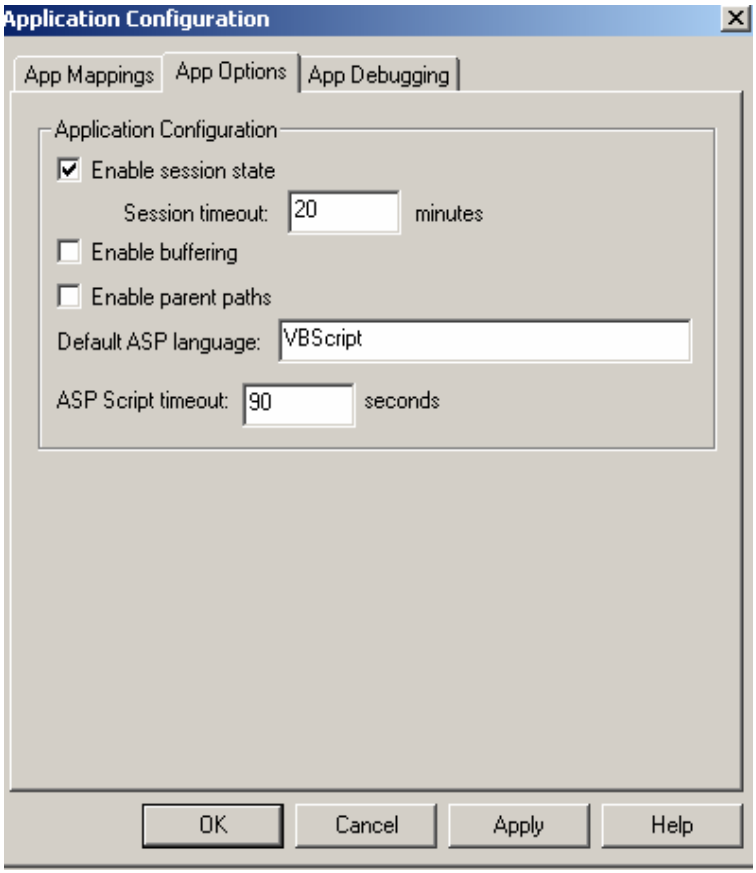
1. Allow anonymous permission to the web server (check the box “allow anonymous access”). In case that it has been decided not to allow anonymous permission remove I_user from the list of accounts that have the permission to log on locally and access the computer from network (this user rights are defined throw local security administrative tool) .
2. In order to allow users from inside the company to authenticate when accessing web server check the box : integrated windows authentication

Default web site / properties /home directory tab /configuration / app mappings tab



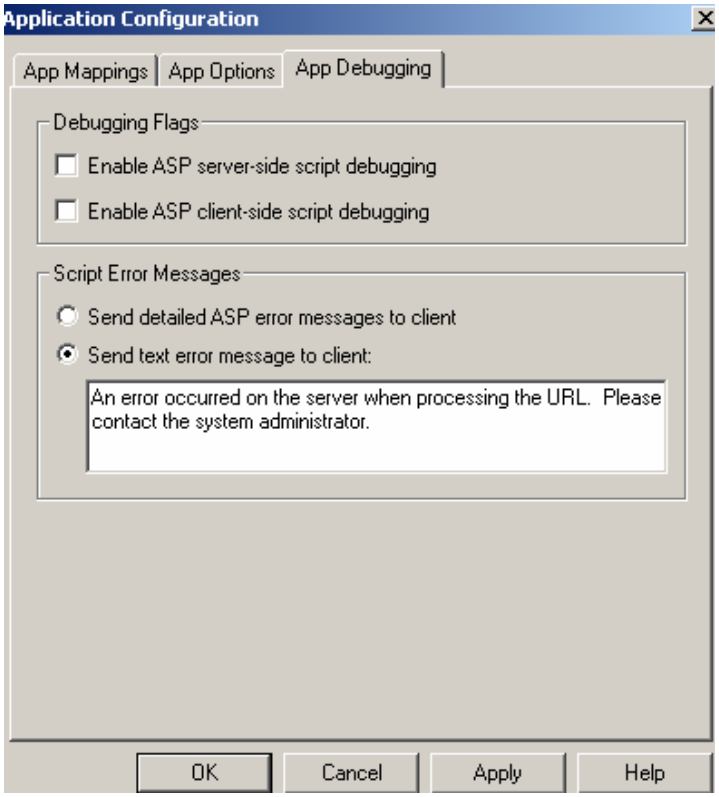
Details can be found at pages 17-18 this document.

Default web site / properties /home directory tab /configuration / app options



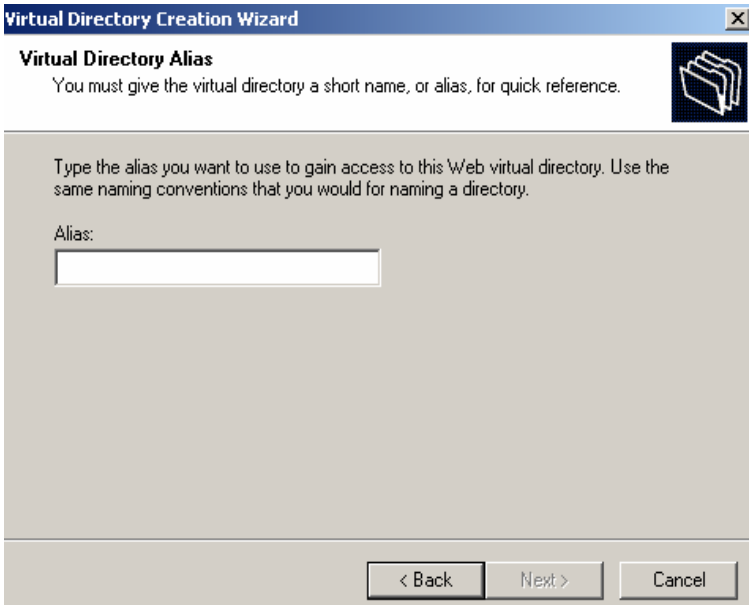
1. Unchecked the box “enable parent paths” .
2. Minimize session time (15-20 minutes)

Default web site / properties /home directory tab /configuration / app debugging



Check the option : " send text error massage to client " this option is recommended because you can define an ordinary massage to remote client when an error accures. A detailed ASP error massages would help potential hackers to gather information about the scripts that are running in the server .

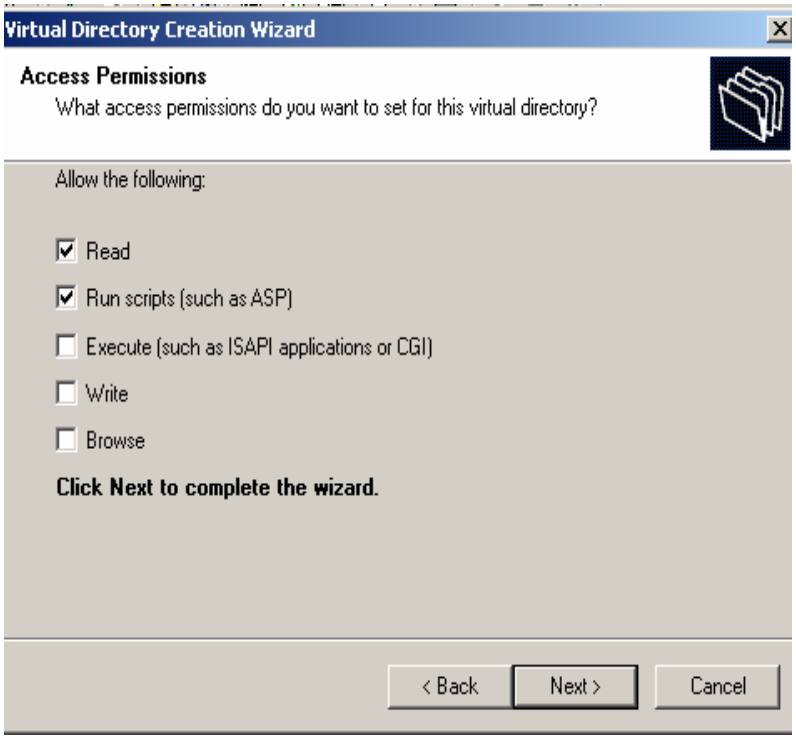
Virtual dierctories security



1. The path of the virtual directories should point the content of the dierctory and not the phisical path in the hard disk , this name should be logical .

2. Create the virtual directory at partition formated with NTFS .

Access permissions



Define read and run scripts permissions. TBD by security system admin if more permissions will be needed.

Set Prevention for Denial of Service and Syn Attacks In The Registry with the following parameters.

Did this by implementing the attached .reg file which people can alter to suit the servers needs.

Use Ipsec policies for defense in depth on the local web server for secondary protection besides the firewall

Just allowed port 80, 21, and 443 in bound past the nic.

Use an IIS application Firewall for defense against any type of Url Vulnerability such as unicode exploit

Use Shadow Enterprise Web Firewall from Safety-Labs at http://www.safety-lab.com/en/products/3.htm. – This product got Rave Reviews.

Disable NetBios From TCP/IP

Do not install microsoft FTP service, If there needs to be an ftp service running , install serv-u ftp server which is a more secureftp server which allows secureftp connections.

Installed FTP serv-u server from http://www.serv-u.com/. This allows secureftp with a lot more configuration than microsoft ftp. Also has its own user database so you don't have to create a local account on the web server.

Test Security On the System

Run a few different security scanners – We use Cybercop 5.5, Internet Security Scanner, Shadow Security Scanner, and Nessusd. It showed zero vulnerabilities. This was accomplished behind the firewall on the dmz vlan

Secure Remote Administration using CYGWIN

Never use just Terminal Services or some kind of other remote administration tool with out using some kind of strong authentication and encryption. Terminal Services has a history of security flaws in the way it does encryption. We suggest using SSH (Secure Shell) which uses a strong type of encryption and that is a protocol then can tunnel any type of TCP connection through. CYGWIN is a unix emulation that resides on top of windows which has SSH support. The cygwin libraries will be actually running your SSH server on the web server. This is not a whitepaper on unix, this is a whitepaper on IIS so if you get a little lost, get a book on Unix.

The Following steps describes how to setup an ssh server on your web server for remote administration.

1. Log on as administrator. Go to http://www.cygwin.com. Select install now

2. Use the explorer to go to the G drive and double click on the cygwin setup program G:\setup.exe. The current version is 2.125.2.10 (February 19th 2002). Click 'Next' and answer the prompts :
    - install from local directory
    - install to c:\cygwin, leave default text file type unix, leave
    - local package directory is G: (whatever drive you mapped in step 1). Click 'Next' default install for All, click 'Next'
    - Install the following list of packages. Double click on the circular arrow to switch the status to skip for packages not in this list.
    - From **Admin**, select all packages.
    - From **Archive**, select unzip and zip packages.
    - From **Base**, select all packages.
    - From **Doc**, select man and newlib.man packages.
    - From **Editors**, select vim package.
    - From **Interpreters**, select perl package.
    - From **Libs**, select regex package.
    - From **Net**, select openssh (openssl) and rsync packages.
    - From **Text**, select groff, less and texinfo packages.
    - From **Utils**, select bzip2, clear, patch and time packages. When you've selected these packages, click 'Next'. The installation tells you whcih packages it is installing as it progresses.

    - Uncheck 'Create desktop icon'. Leave default 'Add to start menu'. Click 'Next'.
    - A post install script runs mkpasswd and mkgroup. Then you should see a message saying 'Installation complete'. Click 'OK'.

3. Edit C:\cygwin\cygwin.bat. Make sure it contains these lines - you will need to add the line setting the CYGWIN environment variable.

```
4.  @echo off
5.  set CYGWIN=binmode tty ntsec
6.  C:
7.  chdir \cygwin\bin
8.
9.  bash --login -i
```

10. Test cygwin to make sure it works. Start, Programs, Cygnus Solutions, Cygwin Bash Shell - should get a command window with a prompt saying 'Administrator@servername'. This is a bash shell and you can use unix or DOS / NT type commands e.g.
    - 'ls /bin' to see the cygwin bin directory
    - 'dir c:' to see the contents of the C: directory

    Type "control d" or 'logout' to exit the shell.

11. If you get a message saying 'cannot create /home/userid', run this command from the cygwin window "mkpasswd -l >/etc/passwd".

12. Run ssh-host-config to set up the ssh host keys and create the sshd_config file in /etc/. You should see output like this:

```
13.  $ ssh-host-config
```

```
14.  Generating /etc/ssh_host_key
15.  Generating /etc/ssh_host_rsa_key
16.  Generating /etc/ssh_host_dsa_key
17.  Generating /etc/ssh_config file
18.  Generating /etc/sshd_config file
19.  Added ssh to /cygdrive/c/WINNT/system32/drivers/etc/services
20.
21.  Do you want to install sshd as service?
22.  (Say "no" if it's already installed as service) (yes/no)
```

Answer 'yes' to the prompt. Press 'Return' to accept the default at the CYGWIN environment question (default

= binmode tty ntsec). The service name is CYGWIN sshd.

23. Type 'cd' to go to your account's home directory. Run ssh-user-config to setup your ssh keys. Create only an SSH2 RSA identity (use a null passphrase - just press return). Output should be similar to this :

```
24.     dellis@nightwatchnss ~
25.     $ ssh-user-config
26.     Shall I create an SSH1 RSA identity file for you? (yes/no) no
27.     Shall I create an SSH2 RSA identity file for you? (yes/no)  (yes/no) yes
28.     Generating /home/pswander/.ssh/id_rsa
29.     Enter passphrase (empty for no passphrase):
30.     Enter same passphrase again:
31.     Do you want to use this identity to login to this machine? (yes/no) yes
32.     Shall I create an SSH2 DSA identity file for you? (yes/no)  (yes/no) no
33.
34.     Configuration finished. Have fun!
```

35. Update the file /home/userid/.ssh/authorized_keys with any keys from other users who you wish to be able to connect to this account. Make sure each entry you add is all on one line.

36. Start the service from the control panel.

37. Test the service from the cygwin prompt using "ssh -v localhost". You will get challenged with the new host key and will have to enter your password as you connect. You can then update the authorized_keys file with the identity.pub file from the user and host you want to connect **from** and test your connection from that host by issuing the command "ssh userid@servername dir c:\" You should see output like this:

```
38.  The authenticity of host 'localhost (127.0.0.1)' can't be established.
39.  RSA key fingerprint is 75:8a:67:20:0d:75:dd:06:64:04:d0:ac:23:c7:74:ba.
40.  Are you sure you want to continue connecting (yes/no)? yes
41.  Warning: Permanently added 'localhost' (RSA) to the list of known hosts.
42.
43.  The last line is:
44.  You are successfully logged in to this server!!!
45.  Now, as long as this is working so far. And your web server is listening on port
     22. Try to connect using SECURECRT (a great ssh client) from your workstation
46.  Now setup securecrt for ssh forwarding. Read the help menu.
47.  Now load up your terminal services client if you have one or what ever remote
     administration program you use and set it to connect to 127.0.0.1 and start
     securecrt so you have an ssh connection with port forwarding
48.  Now fire up Terminal Services client and you should be able to connect to your
     server. Now you have an SSH connection using strong encryption with terminal
     services forwarding through it!!! GOOD JOB
```

49. If You have any problems please refer to this website for help. It is a very good CYGWIN SSH Website - http://tech.erdelynet.com/cygwin-sshd.html

Registry Script

```
Windows Registry Editor Version 5.00

;Written By Dave Ellis, NightWatch Network & Security Solutions dec 27, 2002

;Protection against syn flooding
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPip\Parameters]
"SynAttackProtect"=dword:00000002

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPip\Parameters]
"TcpMaxHalfOpen"=dword:00000100

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPip\Parameters]
"TcpMaxHalfOpenRetried"=dword:00000080

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPip\Parameters]
"TcpMaxPortsExhausted"=dword:00000005

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPip\Parameters]
"TcpMaxConnectResponsRetransmissions"=dword:00000003

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPip\Parameters]
"KeepAliveTime"=dword:00300000

; Enable TCP/IP Filtering
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPip\Parameters]
"EnableSecurityFilters"=dword:00000001

; Disable ICMP Redirect
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPip\Parameters]
"EnableICMPRedirect"=dword:00000000

; 'Disable' IP source routing
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]
"DisableIPSourceRouting"=dword:0000001

; Disallow Fragmented IP
```

```
[HKEY_LOCAL_MACHINE\System\CurrentControlSet\IPFilterDriver\Parameters]
"EnableFragmentChecking"=dword:00000001

; Disable forwarding of fragmented IP packets
[HKEY_LOCAL_MACHINE\System\CurrentControlSet\IPFilterDriver\Parameters]
"DefaultForwardFragments"=dword:00000000

; Disable IP Forwarding
[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters]
"IPEnableRouter"=dword:00000000

; Require PPP clients to authenticated before connecting
[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\PPP]
"ForceEncryptedPassword"=dword:00000002

; Enable RAS logging
[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters]
"Logging"=dword:00000001

; turn off NTFS 8.3 name generation
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Filesystem]
"NtfsDisable8dot3NameGeneration"=dword:00000001

; restrict anonymous connections to ipc$
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA]
"RestrictAnonymous"=dword:00000001

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\LSA]
"LMCompatibilityLevel"=dword:00000004

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application]
"RestrictGuestAccess=dword:00000001

; restrict Null user's and guest access to the Security Event log
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security]
"RestrictGuestAccess"=dword:00000001

; This will restrict Null user's and guest access to the System Event log
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\System]
"RestrictGuestAccess"=dword:00000001

; Disable last logged in user display
;[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
"DontDisplayLastUserName"=dword:00000001
"LegalNoticeCaption"="Warning!"
"LegalNoticeText"="Any Unauthorized Use is Strictly Prohibited"

; Clear page file during system shutdown
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management]
"ClearPageFileAtShutdown"=dword:00000001

; Disable Autorun for the CDROM Drive (1=enabled 0=disabled)
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Cdrom]
"Autorun"=dword:00000000
```