Global Information Assurance Certification Paper

IIS 6.0 – First Steps to Hardening

Jason M. Kraft
June 15, 2004

GSEC Practical – Option 1
Version 1.4b

Abstract

Released as part of Windows Server 2003, Internet Information Server (IIS) 6.0 has made great strides in the security arena. Due in large part to Microsoft's Trustworthy Security Initiative, as well as many embarrassing and widespread vulnerabilities in earlier versions of IIS, Microsoft made the decision to lockdown IIS 6.0 by default. As a result, the latest version installs with most features disabled, a drastic departure from IIS 5.0, which automatically installed with advanced features enabled, often unknown to the administrator.

The question remains however: Is this lockdown enough for a secure IIS 6.0 installation? This paper will briefly address the improvements made to IIS 6.0 "out of the box" and further explore common settings and enhancements needed to secure standard installations. It will also show that in order to make IIS 6.0 more secure, administrators need to implement changes to network settings, system services, access control, and even to the default installation itself. The steps outlined in this paper serve as a primer for hardening IIS 6.0 installations.

Introduction

According to Netcraft, 21 percent of websites surveyed currently run a version of Microsoft's Internet Information Server.[1] While this number seems to imply IIS is a distant second to market leader Apache, it is important to note that Netcraft only accounts for public facing web servers, not the countless others found internally on networks hosting Intranets.

These internal servers, while often overlooked, need to be properly secured as well. Many attack vectors exist, and simply having a firewall in front of an IIS installation is not sufficient. For example, worms can be brought into the network on laptops, thwarting the firewall security policies, or an attacker could exploit a hole that bypasses the firewall. Even more dangerous, and often overlooked, is an employee who launches an attack from inside the network. Predicting how an attack can occur is nearly impossible. With the prevalence of worms and vulnerabilities attacking Microsoft products, locking down all systems proactively is paramount to today's Windows administrator.

Introducing IIS 6.0

Released in 2003, Internet Information Server (IIS) 6.0 sought to address many customer complaints about previous versions. One common criticism was that IIS 5.0 installed and enabled a wealth of features by default, many of which a typical web server did not use. For example, a flaw in the Internet printing service would seem of little concern and not raise alarm, as the service in not widely used. However, unbeknownst to some administrators, this service was enabled, making their sites vulnerable if such a flaw was found.

IIS 6.0 dramatically changed the installation. By default, IIS 6.0 installs with a minimal set of services, serving only static content. All advanced features are disabled, and IIS itself does not install with Windows Server 2003 Standard or Enterprise Edition, a departure from Windows 2000 and IIS 5.0, where IIS was installed by default. Also recently introduced was Windows Server 2003 Web Edition, a scaled down version of Windows Server designed to act solely as web server, removing availability of many system services typically not needed. For instance, Web Edition cannot act as a domain controller.

In addition to the installation changes, the entire IIS 6.0 code base was rewritten with the goal of being more secure. HTTP.SYS, now a kernel mode driver, serves as the core of IIS 6.0. This new implementation removes the need to switch between user and kernel modes (as was the case with IIS 5.0), which in turn improves server performance, as well as security. HTTP.SYS receives requests and then passes them to user-mode processes, never actually running any code. This acts as a buffer, preventing user mode processes from accessing resources in the system kernel and from crashing IIS.[2]

The file system was also tightened. By default, the IUSR_*ComputerName* account (*ComputerName* is the server's NetBIOS name), which is used by anonymous web users, is denied write access to the default IIS source folder, found in C:\Inetpub\wwwroot. Also, users must be a member of the local administrators group to run programs located in the system folder.[3] Access to parent paths are also disabled to prevent directory traversal attacks. Parent path access is often achieved by inserting ".." into a command, or as was case with previous versions of IIS, inserted into a URL and exploited remotely.

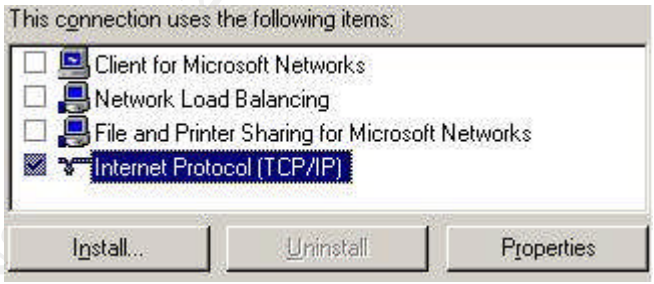
An important note before continuing: test, change a setting, and test again. This should be the manner in which an administrator proceeds when locking down IIS. Proceeding cautiously with this rigorous approach will allow one to easily identify which changed setting broke functionality.

Hardening Network Settings

In order to secure a server of any kind, proper network settings need to be applied. On a public web server, this becomes even more critical. Ideally, the web server(s) will be behind a firewall, but as demonstrated earlier, while a firewall is a vital part of any defense, it is not enough. Before installing IIS on the server, the network settings should be hardened against potential attacks.

To change the network settings on a Windows 2003 server:

1) Open the **Control Panel**, and then select **Network Connections**
2) Right-click on **Local Area Connection** and select **Properties**

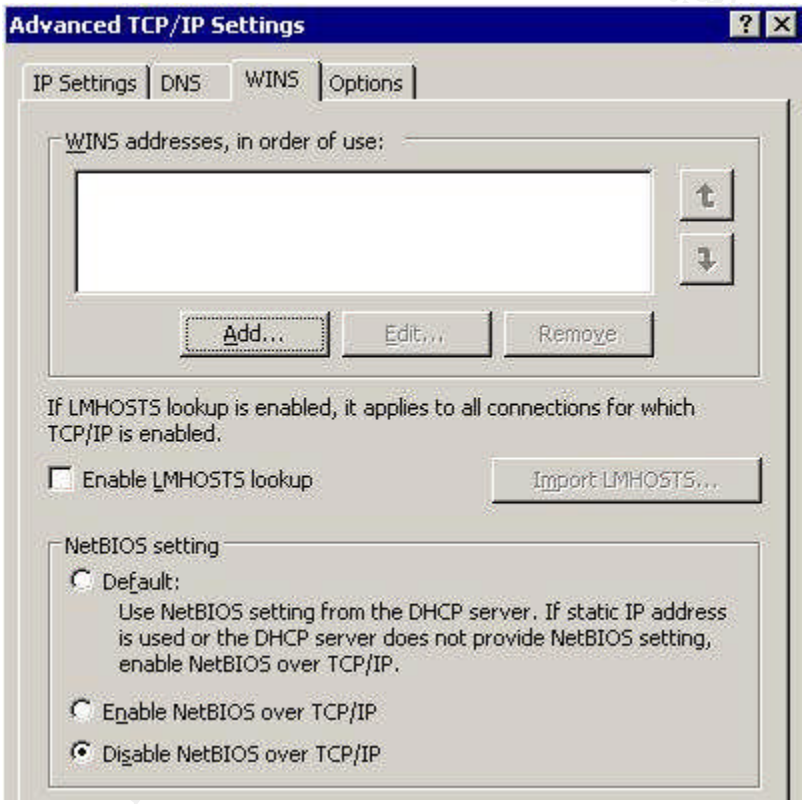


Remove all protocols from the server except TCP/IP, as all other services provide potential weakness to be penetrated. Uncheck *File and Printer Sharing for Microsoft Networks* and *Client for Microsoft Networks* on the network adapter assigned to your public IP address (These protocols are not installed when using 2003 Web Edition.) If the server has only one network adapter, you may be able to uninstall the protocols completely. Installing or uninstalling a protocol affects all adapters present on the system, so deselecting protocols on appropriate adapters is important. For a server behind a firewall, the firewall will also help mitigate the risk of keeping these protocols enabled. However, since the protocols will not be used, they should be disabled to remove the SMB protocol from the adapter.

To access advanced TCP/IP Properties:

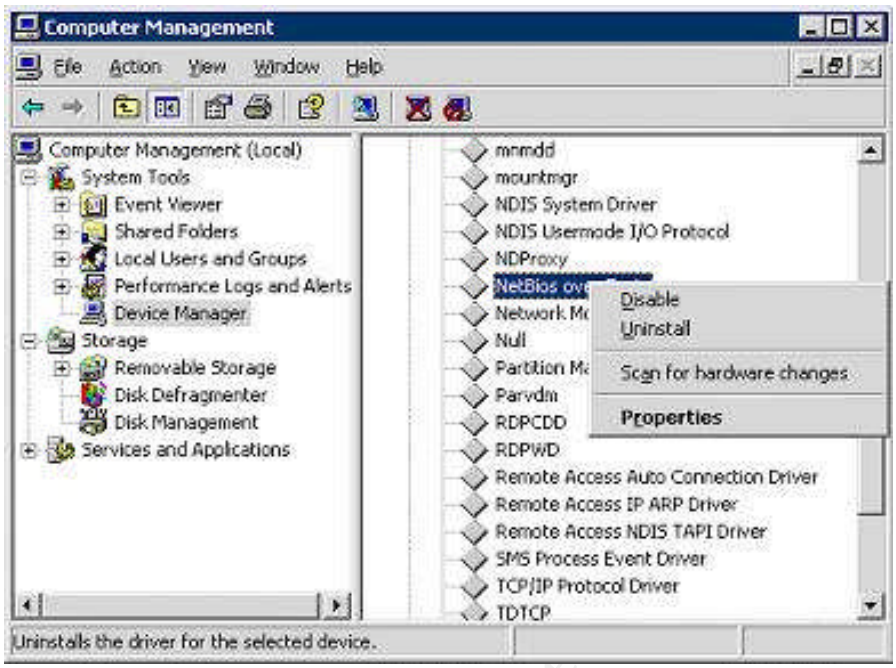
1) Select **Internet Protocol (TCP/IP)** and select **Properties**
2) Select the **Advanced…** button

Under the WINS tab, uncheck *Enable LMHOSTS lookup* and choose *Disable NetBIOS over TCP/IP*. As NetBIOS has historically been a popular service to exploit on Windows operating systems (server and desktop), disabling is mandatory. Most recently, Microsoft Security Bulletin MS03-34 warned of an information disclosure vulnerability in the NetBIOS service.[4]



In addition to the above method of disabling NetBIOS, Microsoft recommends to disable the service using Device Manager: [5]

1) Right-Click on **My Computer** and select **Manage**
2) Click on the **Hardware** tab, open **Device Manager**, click on **View**, and select **Show hidden devices**
3) Expand **Non Plug and Play Drivers**
4) Disable **NetBIOS over TCP/IP** by right-clicking and selecting **Disable**



In addition to these steps, some advanced hardening should be done on the TCP/IP stack itself. Microsoft Knowledge Base Article 324270 details the following steps that can be taken on a Windows 2003 server to lessen the risk against Denial of Service (DoS) attacks.[6]

To access the registry and add a value:

1) Click on **Start** and then **Run**
2) Type **Regedit** and press **OK**
3) Drill down the options on the left until reaching the appropriate container, as specified below
4) Highlight the key in the left pane
5) Select the **Edit** menu option, and then **New…DWORD Value**

1) Improved SYN Attack Protection
   A SYN attack occurs when a SYN ACK packet is sent to a host rather than a SYN packet, which is expected. The server tries to respond with an ACK packet. Since the source address is spoofed, the server overloads while trying to respond to these requests, and is thus unable to fulfill legitimate queries. Altering the registry value outlined below will cause connections to time out more quickly during such an attack.

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
   REG_DWORD value **SynAttackProtect**
   Recommended Value: **1**

2) Enable Dead Gateway Protection
   When a DoS attack occurs, the system's default gateway can become

swamped with requests and stop responding. By default, Windows has the ability to switch to a backup gateway. If in the midst of a DoS attack, the backup gateway is likely to become unresponsive as well.[7] Disable switching to another gateway with this key.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
REG_DWORD value **EnableDeadGWDetect**
Recommended Value: **0**

3) Enable Path Maximum Transmission Unit Discovery
As different devices on the network accept differing packet sizes, TCP attempts to determine the maximum transmission size (MTU) of a remote host. This causes more network traffic as packets may need to be split into smaller sizes. By leaving this setting enabled, an attack could occur where the MTU size is very small, causing the host to become overworked.[6]

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
REG_DWORD value **EnablePMTUDiscovery**
Recommended Value: **0**

4) Shorten the Keep Alive Packet Transmission
After a connection to a host is established, TCP/IP will send a keep-alive packet at a specified interval in order to test connectivity. If the remote computer drops a connection without telling the other, it will be two hours (by default) before the host learns about the dropped connection. Microsoft recommends changing this wait to 5 minutes.[6]

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
REG_DWORD value **KeepAliveTime**
Recommended Value: **300,000** (time in milliseconds)

Additionally, Microsoft recommends the following keys be added to further harden the TCP/IP stack. [8]

5) Allow ICMP Redirects to Override OSPF Routes
The timeout value for ICMP redirects is 10 minutes by default, and can cause a black hole condition where traffic is improperly routed. Disable ICMP redirects to allow OSPF to handle all routing.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
REG_DWORD value **EnableICMPRedirect**
Recommended Value: **0**

6) IP Source Routing Protection
IP source routing allows a computer to specify a route for the packet to take, thus potentially allowing an attacker to mask their true location. Setting this registry value to 2 will cause all source routed packets to be dropped.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
REG_DWORD value **DisableIPSourceRouting**
Recommended Value: **2**

7) Decrease Time for TCP/IP to Close Connections
This key will shorten the time it takes for the TCP/IP stack to clean up half-open connections. A value of 2 or greater causes the stack to internally use SYN attack protection. Values of 1 and 0 are also valid, but a value of 0 will be very short, and distant remote hosts may not respond before the connection is closed.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
REG_DWORD value **TcpMaxConnectResponseRetransmissions**
Recommended Value: **2**

8) Decrease Retries of Unacknowledged Data
To mitigate a SYN flood attack, decrease this parameter from the default of 5 to 3. In this way, the stack will stop retransmitting data that it receives no response to at 3, in effect closing improper TCP/IP sessions sooner.

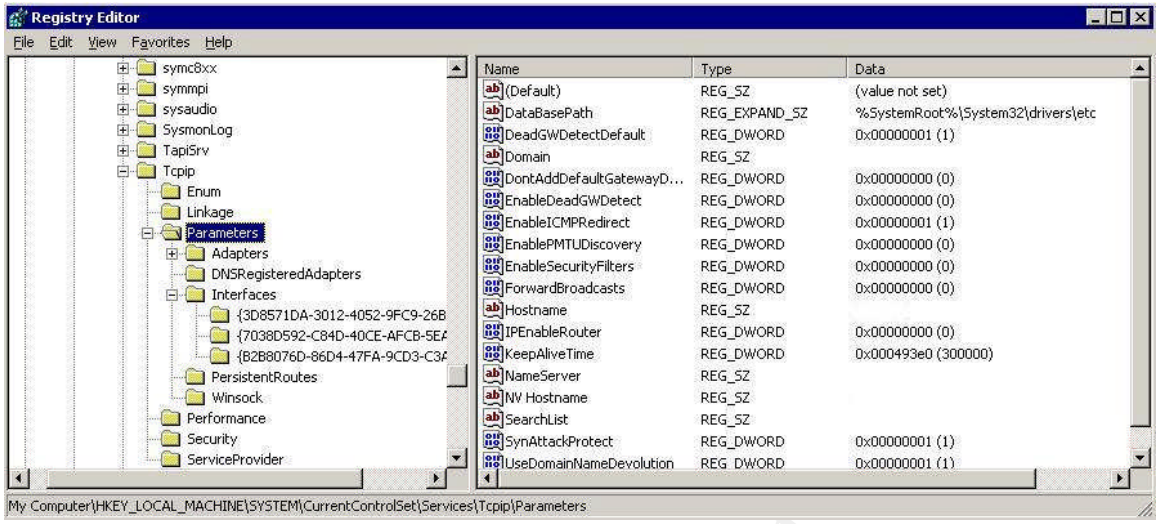
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
REG_DWORD value **TcpMaxDataRetransmissions**
Recommended Value: **3**

9) Disable Default Gateway Discovery
This key enables Internet Router Discovery Protocol (IRDP), which will automatically detect and configure a default gateway address. Set this value to 0 in order to disable IRDP.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
REG_DWORD value **PerformRouterDiscovery**
Recommended Value: **0**

10) SYN Attack Protection after Dropped Connections
This value specifies when SYN attack protection should begin based on the number of dropped connections.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
REG_DWORD value **TcpMaxPortsExhausted**
Recommended Value: **5**

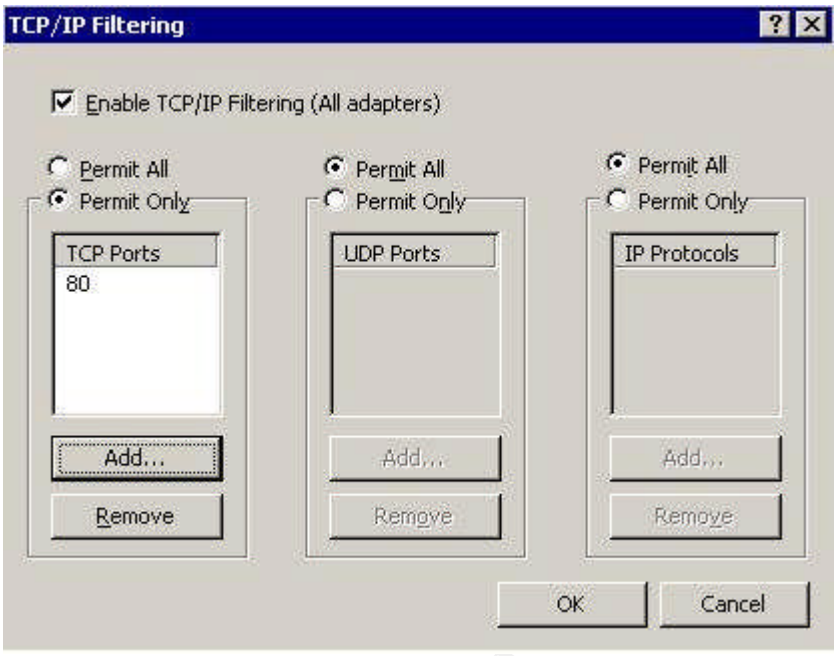


IIS 6.0, like its predecessor, has socket pooling enabled. This feature allows IIS to listen on all server addresses simultaneously. For instance, if you are running two web sites, each with its own IP address and hosted on the same server, IIS will listen on a shared socket pool that encompasses all addresses on the system.[9] Socket Pooling is shown as an IP address of 0.0.0.0 when issuing a **netstat –na** command on the IIS server. Left enabled, it can potentially pose problems with secure sites or domains that should not be exposed on the same listener.

To disable socket pooling in IIS 6.0, install and run httpcfg.exe, which is found in the Support/Tools folder on the Windows Server 2003 CD. IIS 6.0 uses an inclusion list for listeners, but by default listens for all addresses. To disable socket pooling, each individual IP address needs to be added to the inclusion list as follows: [10]

1) Open a **command prompt** and navigate to where httpcfg.exe was installed
2) Type: **httpcfg set iplisten -i aaa.bbb.ccc.ddd** (IP address to add.)
3) When completed, this status message is shown: *HttpSetServiceConfiguration completed with 0*

Port filtering also increases server security. Even if the server is placed behind a firewall, locking down access to ports is part a defense in-depth strategy. Extra care must be taken when using port filtering, as it is easy to cripple server functionality by filtering the wrong ports, or ports needed for network communication. HTTP access typically uses TCP port 80, so this port should normally be permitted. However, only allowing TCP port 80 access will restrict the server from other functions. If the server needs to serve SSL encrypted web pages, TCP port 443 traffic should be allowed as well. It is important to note that port filtering only applies to inbound traffic. The server will still be able to establish outbound connections on alternate ports.



System Services

The next step in locking down an IIS 6.0 web server is to disable unneeded system services. Services that are unnecessary for server operation should be removed, or at minimum disabled. Disabling services reduces the attack surface of the server, thus decreasing potential exploits. While setting the startup type to manual prevents the service from starting with the system, it does not prevent another operating system service or device driver from starting it. When a service is disabled, an administrator is required to change the startup type to manual before that service can be started. [11]

When disabling services on a high risk server, the goal is to leave only essential services running. While targeting services that have known vulnerabilities is important, and even a priority, it should not stop there. Seemingly benign services left running on a server can be exploited in the future. For instance, while the Automatic Updates service may not have any known weaknesses at present, it should nonetheless be disabled to lessen the impact of a flaw discovered at some future point.

The following services have an automatic startup type and should be disabled if not needed: [11]

Automatic Updates	Used for automatic downloading of critical updates
Computer Browser	Maintains list of computers on the network, not necessary for a web server
DHCP Client	A server will likely have a static IP address, so the DHCP client is not needed
Distributed File System	Manages volumes that are spread across a LAN or WAN

Distributed Link Tracking Client	Maintains links between NTFS files across the network
Distributed Transaction Coordinator	Manages information distributed across numerous computer systems, such as SQL databases or message queues
Error Reporting Service	Sends feedback and debugging information to Microsoft
Help and Support	Microsoft Windows help system
IPSEC Services	If not using IPSEC, this can be disabled
Plug and Play	Installs hardware automatically. As server hardware rarely changes, this can be disabled
Print Spooler	Printing services are rarely needed from a secured web server
Remote Registry	Enables registry changes from over the network. Registry changes can be made from the console when necessary
Secondary Logon	Allows use of the Run As command, a potential tool for an attacker to elevate credentials
Server	Provides RPC sharing, as well as file and print sharing over the network. This service can likely be disabled if the server if solely running IIS
TCP/IP NetBIOS Helper	Provides help for NetBIOS resolution to clients. NetBIOS should be disabled, so this service should be as well
Wireless Configuration	Auto Configuration for 802.11 adapters

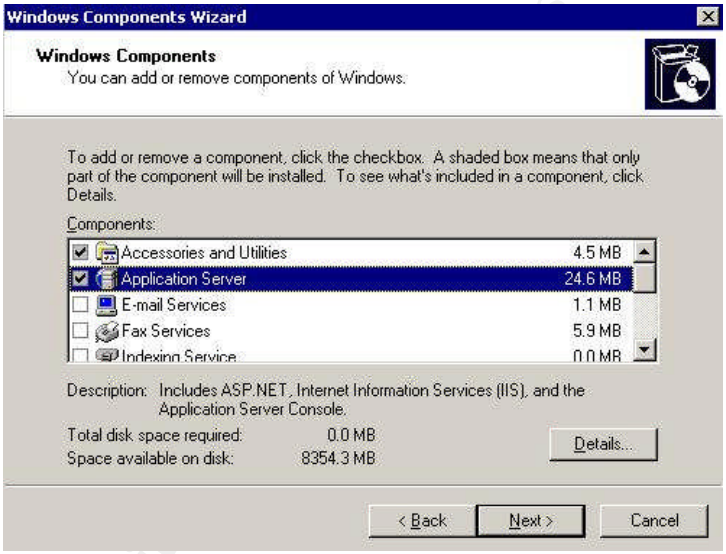
These services have a manual startup type and can typically be disabled if not needed:

Application Management	Works with Add/Remove Programs in the Control Panel
Background Intelligent Transfer Service (BITS)	Used with Automatic Updates to throttle download speeds
Distributed Link Tracking Server	Tracks information about NTFS based file moves across the domain
Fax Service	Sends/Receives faxes
File Replication Service	Enables file synchronizations over different servers
Indexing Service	Indexes files to provide faster search capabilities
NetMeeting Remote Desktop Sharing	Provides remote administration through NetMeeting
Remote Access Auto Connection Manager	Provides alternate methods to connect; used with VPN or dial-up connections
Remote Access Connection Manager	Manages VPN or dial-up connections from the web server to the Internet or other servers
Remote Desktop Help Sessions Manager	Manages Remote Assistance sessions
Removable Storage	Manages removable media and operates tape libraries or jukeboxes
Telephony	Controls telephony devices and IP-based voice connections
Terminal Services	Used for remote administration
Uninterruptible Power Supply	Manages an uninterruptible power supply device through the serial port. Can be disabled if not used.
Upload Manager	Uploads driver information to aid in finding drivers and support over the web
Volume Shadow Copy	Creates snapshot backups for easy restores

WinHTTP Web Proxy Auto-Discovery Service	Allows for an HTTP client to automatically discover a proxy configuration
Windows Installer	Allows programs to be added/removed from the server. Disable for heightened security, but may be needed for application installations
WMI Performance Adapter	Provides performance information to WMI providers over the network

Installing IIS 6.0

As it no longer installs as part of the default operating system (except when installing Windows Servers 2003 Web Edition), IIS 6.0 will need to be installed through Add/Remove Windows Components, located under the Control Panel in Add/Remove Programs. To install IIS and its components, check Application Server, and then choose Details…



As illustrated by the following table, IIS 6.0 installs with a minimum set of components enabled as compared to its predecessor. [12]

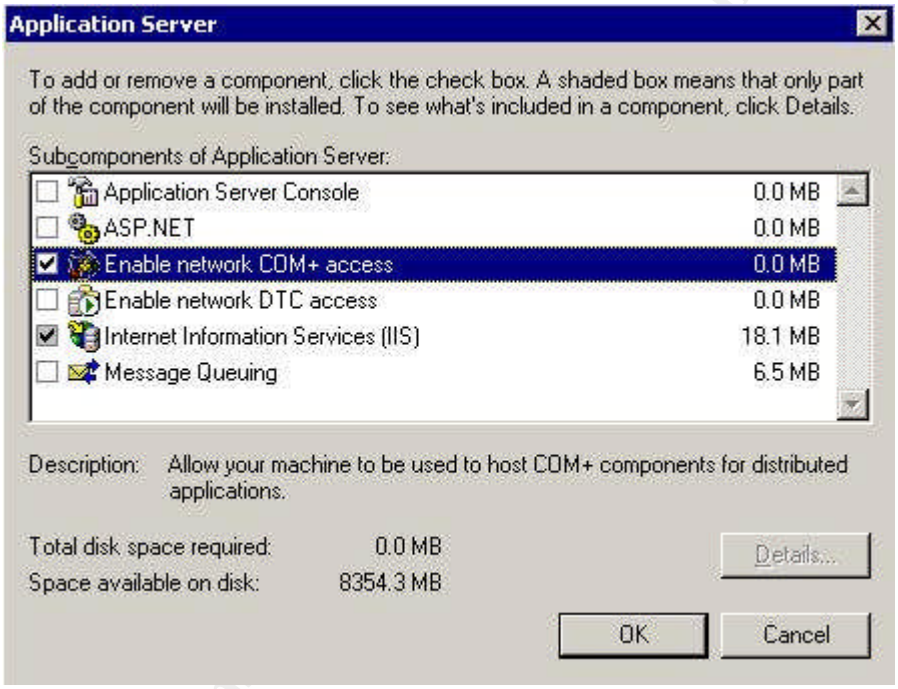
IIS Component	IIS 5.0	IIS 6.0
Static File Support	Enabled	Enabled
ASP	Enabled	Disabled
Server-side Includes	Enabled	Disabled
Internet Data Connector	Enabled	Disabled
WebDAV	Enabled	Disabled
Index Server ISAPI	Enabled	Disabled
Internet Printing ISAPI	Enabled	Disabled
CGI	Enabled	Disabled
FrontPage Server Extensions	Enabled	Disabled
Password Change Interface	Enabled	Disabled
SMTP	Enabled	Disabled
FTP	Enabled	Disabled
ASP.NET	N/A	Disabled

BITS	N/A	Disabled

While IIS 5.0 installed everything and relied on the administrator to disable what was not needed (resulting in many services running that were not necessary), IIS 6.0 takes the opposite approach. As such, it is important to take time to identify and enable only the necessary components. It would be foolish to enable everything just to "get up and running quickly".

Let's examine each major choice presented at installation, as well as the options for each.

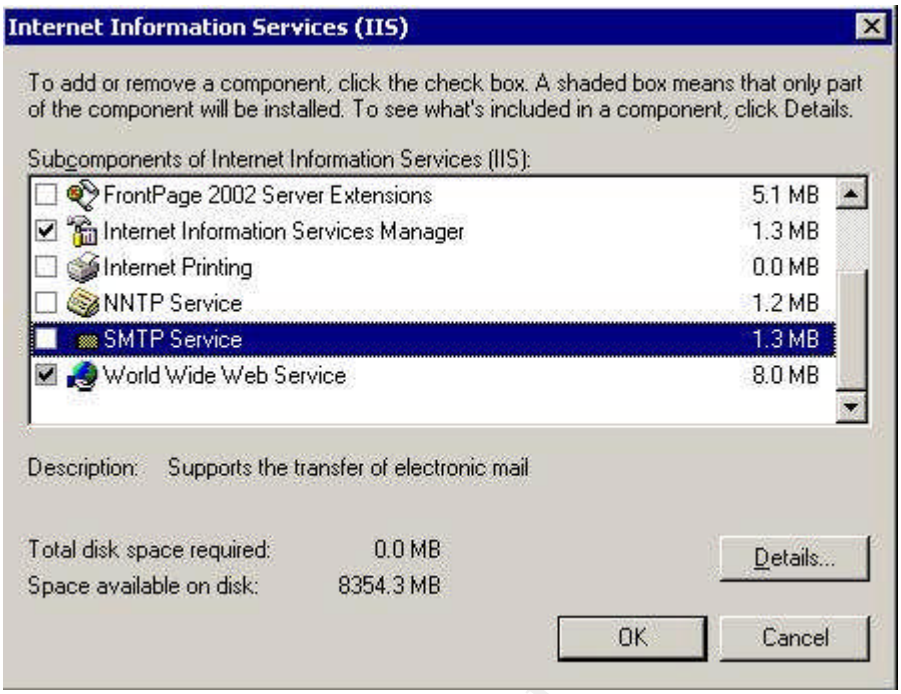
Application Server Options:



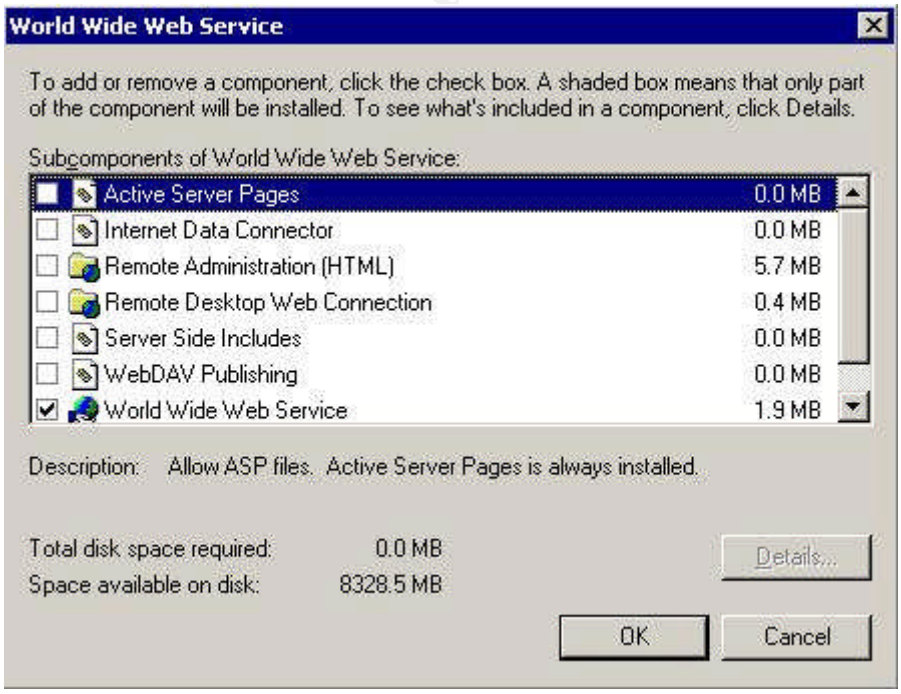
Of these top level options, Application Server Console, Enable network COM+ access, and Internet Information Services (IIS) are enabled by default. A grey checkbox indicates only a subset of available components is installed, as is shown above with Internet Information Services. On a dedicated web server, administrators can uncheck Application Server Console, as IIS Manager will be used instead.

Let's also look at the top level options available when installing Internet Information Server. IIS 6.0 has a subset of components to install, most of which are disabled by default.

Internet Information Server Options:



Selecting World Wide Web Service and clicking Details brings up the following options:



One of the most important choices to make after an installation, and before creating web sites, is the location for the wwwroot directory, where the web site source files reside on the local server. IIS will make the home directory of any new site C:\inetpub\wwwroot. While a default, it is nonetheless important to

move this folder to a different partition. Moving the wwwroot folder to another volume prevents IIS from filling the system drive with data and shutting down the operating system.

1) Open **IIS Manager**
2) Expand <server name>, and then expand **Web Sites**
3) Right-click and select **Properties** on the web site you wish to change
4) Select the **Home Directory** tab
5) **Local Path:** indicates the location for source files on the local system This should be located on a separate partition than the system files

Moving the location of web site source files prevents directory traversal attacks on the system. An example of a dangerous directory traversal is:

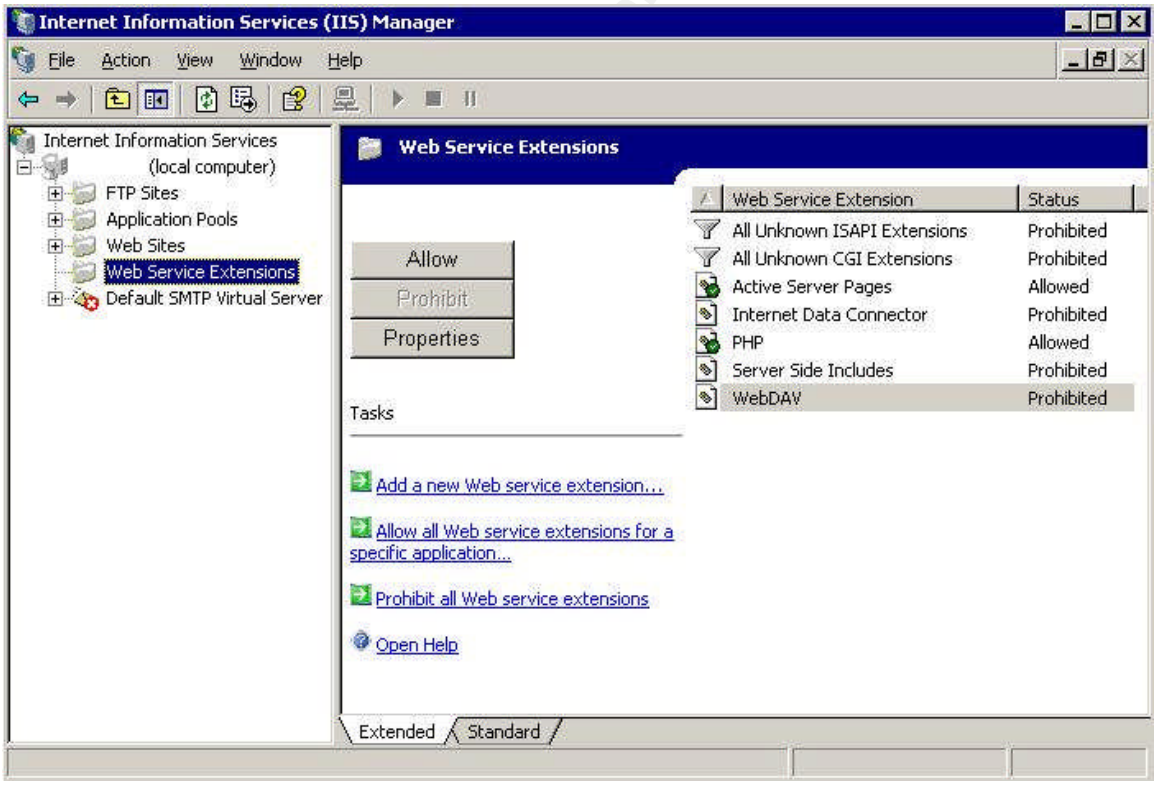
http://www.yourwebsite.com/../../Windows/System/cmd.exe.

An exploit like the one above (although this isn't a working example) was announced for IIS 4.0 and 5.0 servers in Microsoft Security Bulletin 00-078.[13] An attacker could remotely execute programs on the web server with IUSR_*ComputerName* account permissions. The IUSR_*ComputerName* account was part of the Everyone group, which had permissions on the system folders. The "/../" in the URL above changes the current directory to the one immediately above it. In this way, a URL with enough "/../"s could back up from the wwwroot directory all the way to the root directory, and then proceed forward to the system folder. An attacker only needed to know how to craft the malicious URL, an easy task as a default Windows installation is well known. While this could be possible under a default IIS 6.0 installation, moving the home directory to another partition mitigates this risk, as there are currently no known ways to traverse partitions. [14]

Soon after installing, IIS 6.0 will present a lockdown security wizard. This is a good place to begin, as it will quickly allow the administrator to enable or disable desired features. The IIS Security Lockdown Wizard will present you with four

services to set startup properties on: HTTP, FTP, SMTP, and NNTP. Service startup options are Automatic, Manual, and Disabled. This wizard offers the same capabilities as going to Services and setting them manually. Also present in this wizard is the ability to turn on more advanced features for the server (remember that only static content can be served by default). Here administrators can enable ASP.NET, FrontPage Server Extensions, and CGI Handlers, among other things. [15]

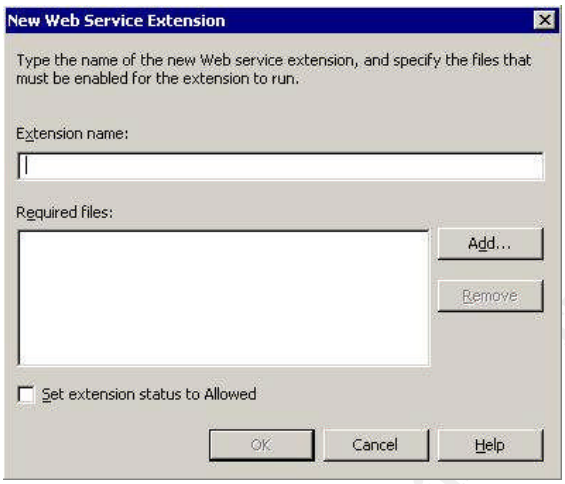
If an administrator chooses not to run the Lockdown Wizard, or more likely, needs to add features at a later time after installation, advanced services can be enabled from the IIS Manger console. Expand the server name (local computer) and then select Web Services Extensions to enable. Allowing or prohibiting access to Active Server Pages or Server Side Includes is as easy as highlighting the service and clicking allow. Services such as PHP support can be added here as well. Clicking "Add a new web service extension" allows administrators to browse to the file that supports the extension. For PHP support, the required file is php4isapi.dll. By default, IIS 6.0 keeps extensions in C:\Windows\system32\inetsvr. For ease of administration it is recommended that all extensions be located together, if possible.



To add a new extension:

1) Open **IIS Manager** and select **Web Services Extensions.**
2) To enable an existing extension, highlight the extension and click **Allow**
3) To add a new extension, click **Add a new Web Service Extension.**

4) Type an appropriate display name for **Extension Name**, and click **Add...** to browse to the .exe or .dll of the component.



On an ASP enabled installation, a potentially dangerous installed component is called FileSystemObject. This scripting component, which can be called from the Windows Script Host or from an ASP page, has the ability to interact with the file system. Creating, modifying, and deleting files are all within the capabilities of this component. If an attacker gains limited access to the server, he or she might be able to use this object against files on the system. As always, test application functionality after making this change. [5]

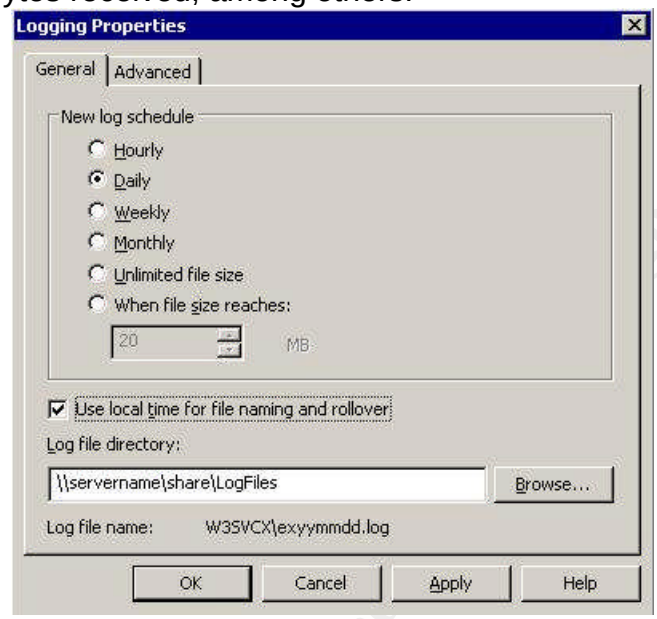
1. Open a **command prompt**
2. Change to the **C:\Windows\system32** directory
3. At the command prompt, type **regsvr32 scrrun.dll /u** and then press Enter.
   The following message appears:
   DllUnregisterServer in scrrun.dll succeeded

Lastly, the location of the IIS log files should be changed. For a highly secure web server, this location should be over the network to a remote system. IIS logging supports Universal Naming Convention (UNC) names for remote shares as well as ODBC logging to a SQL database. In this way, an attacker who compromises the system won't have access to the log files to cover his or her tracks, and all logs can be centralized for easier review and backup.[14] Each website has its own separate log which can be customized, so choose which options are pertinent for each specific site, then relocate the log file by using IIS Manager.

To change the location of IIS log files:

1) Open **IIS Manager** and right-click an individual website, or choose the top level **Web Sites** to move the log files for all web sites on the server
2) Under the **Web Sites** tab, logging should be enabled and using W3C format by default. Click **Properties**.

3) **Log File Directory**: enter the network path to where the log files should be kept.
4) The Advanced tab allows for more detailed logging options, such as bytes sent and bytes received, among others.



System Access Control

To this point, we hardened the Operating System Services, TCP/IP settings, and installed IIS with a minimal set of services. The final critical element for IIS security is access control, including user accounts, access rights, and group policy settings.

The Guest account, which has caused problems in the past for Windows servers, is disabled by default. Renaming accounts does not have a significant security benefit, as built-in Windows accounts have well known Security Identifiers (SID), and many tools exist to obtain this information. For example, the local administrator account SID ends with -500, so renaming the account to *newadmin* will help thwart the more basic attacks, but not deter those that are more advanced. Renaming an account does not change the underlying SID.

Nonetheless, leave the Guest account disabled and rename both the local Administrator account and IUSR_*ComputerName* account. After renaming the IUSR_*ComputerName* account, change the metabase in order to allow access from the renamed account.

1.Open **IIS Manager**.
2.Right-click the ***<servername>*(local computer)**, and then choose **Properties**.
3.Select the **Enable Direct Metabase Edit** check box, and then click **OK**.
4.Browse to the location of the **MetaBase.xml** file, by default **C:\Windows\system32\inetsrv**.

5.Right-click the MetaBase.xml file and then click **Edit**.
6.Search for the **AnonymousUserName** property, and type the new name of the IUSR account.
7.On the File menu, click **Exit**, and then click **Yes**.[5]

Renaming and disabling accounts is not enough. Proper permissions also need to be assigned to all accounts on the system. First and foremost, all drives should be formatted with NTFS. The root drive, which holds the operating system files, should contain only these files if possible (as illustrated earlier). Remove the default permissions on this volume, which for the Everyone group defaults to read and execute. Only the Administrator and System accounts need access to the System Volume.[5]

Once each directory is created, it is important to examine the effective permissions. For a typical website, the IUSR_*ComputerName* account should have read and execute permissions, while an administrator account should have full control over the files and folders. It is crucial that web site permissions, set within IIS Manager, be used in conjunction with typical NTFS permissions. NTFS permissions apply only to those accounts with specified access to a file or folder, while web site permissions apply to everyone who accesses the site. When a conflict arises, the most restrictive setting is the effective one. The following tables outline both NTFS and Web Site Permissions. [14]

NTFS Permissions (Recommended)

CGI Files (.exe, .dll, .cmd, .pl)	Everyone – Execute Administrators – Full Control System – Full Control
Script Files (.asp)	Everyone – Execute Administrators – Full Control System – Full Control
Include Files (.inc, .shtm, .shtml)	Everyone – Execute Administrators – Full Control System – Full Control
Static Content (.txt, .gif, .html)	Everyone – Read Only Administrators – Full Control System – Full Control

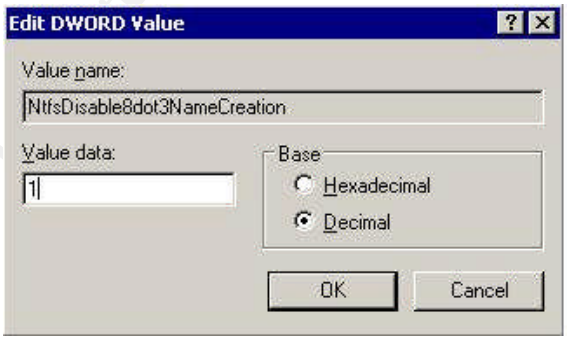
Web Site Permissions

Read	Default setting, Users can view content
Write	Files can be changed by users

Script Source Access	Read: Users can view source Write: Users can change source Allowing users to view script source code could expose sensitive data, such as passwords
Directory Browsing	Users can views lists and collections
Log Visits	All visits are logged
Index this Resource	Allows for faster searches
Execute	None: No scripts or executables can be run by users Scripts Only: Users can run scripts Scripts and Executables: Users can run scripts and executables

In addition to file permissions, consider disabling support for 8.3 format filenames. Windows auto-generates these smaller names for backwards compatibility with 16-bit applications. For example, a file named *thislongfile.txt* can be accessed on the server with *thislo~1.txt*. This shorter name may aide an attacker in accessing unknown files on the server. The result of changing this key is to make files more difficult to locate for an attacker.[8]

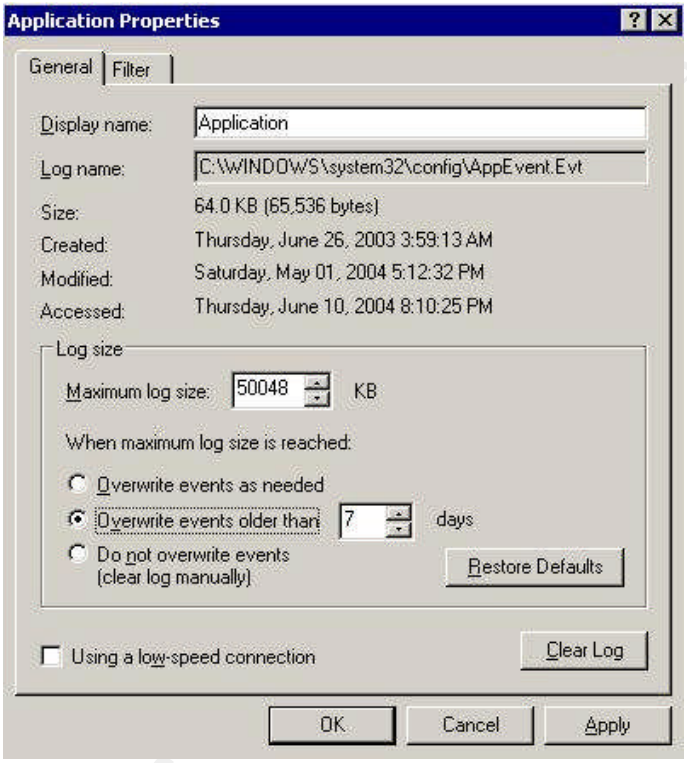
1) Open the **Registry Editor**
2) Navigate to: **HKEY_LOCAL_MACHINE\ System\CurrentControlSet\Control\FileSystem**
3) Select **NtfsDisable8dot3NameCreation**
4) Change the DWORD value to **1 (decimal)**



Before discussing policies and auditing, the system log files should be addressed. By default, the Application, Security, and System event logs are kept in C:\WINDOWS\system32\config, and named AppEvent.Evt, SecEvent.Evt, and SysEvent.Evt, respectively. On a domain member server, these settings can be set using group policy. However, in this case, we will set them manually as if it was a stand-alone server.

To access the event log properties:

1) Open the **Event Viewer**, located in **Administrative Tools**
2) Select an Event Log (**Application, Security,** or **System**), right-click and choose **Properties**. Properties are set on each individual log.
3) Maximum log file size must be set in increments of **64**



1) Log Size:
   This is perhaps the most important event log setting to change. By default, all 3 log files have a maximum size of 16 MB, and are also set to overwrite events as needed.

   Microsoft only recommends increasing the security log size from the default to 81 MB[16], but all three should be made larger to some degree. The practical limit on all 3 log files (in total) is less than 300 MB, as current limitations in the Windows architecture affect performance and cause log file fragmentation.[17] Set all three log files to about 50 MB (50,0048 KB) to begin with, and then adjust the size as needed.

2) When maximum log file size is reached:
   Overwrite events as needed (the default)
   Overwrite events older than X days
   Do not overwrite events (clear log manually)

Which option to choose depends on the environment and company policies in place regarding logging. The log files should be backed up for historical reasons and the log overwrite policy should be based on how quickly the logs fill up and how often they are backed up. If the backup policy calls for a backup every 7 days, then the logs can be set to overwrite as needed every 7 days as well. More sensitive web sites may need to be backed up on a daily basis. The key point to remember is an event log should never be overwritten without a backup having been made.

To help monitor event log size, especially in relation to total size available, a registry change can be made to log an audit event when a specific percentage is reached. For example, if the registry value is set to 80, an event will be logged when the log file reaches 80 percent of available file size. This setting will allow the administrator to better tune log file sizes, as well as potentially remedy a situation where the event log could be overwritten. If the log file is set to *overwrite events as needed* this audit event will not be generated.[8]

1) Open the **Registry Editor**
2) Navigate to **HKEY_LOCAL_MACHINE\ SYSTEM\CurrentControlSet\Services\Eventlog**
3) Select **Application**, **Security**, or **System**
4) Select the **Edit** menu option, then **New…DWORD Value**
5) Value name: **WarningLevel**
6) Value Data: **0-100** (number represents percentage threshold at which event will log)
7) Repeat for each individual log file

In addition to these access control methods and system log settings, consider using group policy to set security policies. When the server in question is not a domain member, many of the same benefits can be found by using the local security policy. Setting permissions and rights using a policy has the benefit of being reapplied at regular intervals. As such, a change made by an attacker or a fellow administrator will be reset to the desired value at the next policy refresh. Also, a newly introduced server can have the same Group Policy Object applied, easing administration and creating a uniform security environment. Launch the Local Security Policy editor from the Administrative Tools folder.

Account Policies

If running an FTP site or perhaps a password-protected web site, it is necessary to set account policies. These policies set restrictions on a system's user accounts through specific password options. Password minimum/maximum age, password history, and complexity requirements are all defined here. Account lockout policy can also be set, as well as how to deal with potential brute force attacks.

1) Password Policy

Enforce password history – 12 passwords remembered
The number of passwords that need to be used before the user is allowed to repeat one used previously.

Password must meet complexity requirements – Enabled
Passwords must contain upper and lower case letters, as well as numbers or non-alphanumeric numbers.

Minimum password age – 5 days
How many days a password must be in effect before it can be changed. A setting of 5 days is usually sufficient, as the user adapts to the new password.

Maximum password age – 30 days
Number of days a password is valid before the user must change. In high security environments, 30 days is often recommended.

Minimum password length – 8 characters
Minimum characters allowed for passwords. This number should be at least 8.

2) Account Lockout Policy

Account Lockout Duration – 60 minutes
This setting, in minutes, will lockout the account, preventing user access. A value of 0 would cause an administrator to manually unlock the account. In some cases, a value of 60 will suffice. This policy greatly hinders brute force attacks on passwords.

Account Lockout Threshold – 5 invalid logon attempts
The number of incorrect password attempts allowed until the account is locked out. This value should be high enough that legitimate password typos typically don't lock the account, usually 5.

Reset account lockout counter after – 120 minutes
The number of minutes after which the invalid password counter will reset. Typically this can be set at 120 minutes.

How many bad password attempts should be allowed until the account is locked out? Does the account need to be unlocked by an administrator, or will it reset after a certain number of minutes? While a basic guideline was presented here, these are the questions that will need to be answered by, and based, on a company's security policies.

Local Policies

1) Audit Policy

When properly set, audit policies can identify who had access to what, and when. This information is especially relevant when reviewing server logs. For each option, administrators can log success, failure, or both. However, excessive auditing may hurt server performance.

Audit account logon events – Success/Failure
By default, this option will log success events, but for a web server, logon failures will provide a better picture as to who is trying to access the server and with which account.

Audit account management – Success/Failure
This option should be set to log both success and failure events. User accounts created or deleted, as well as password changes, will be logged.

Audit logon events – Success/Failure
By default, this option will log success events, but failure events should be logged as well. This will show which accounts are accessing the server, and logging failures in a high risk environment (such as a web server) is recommended.

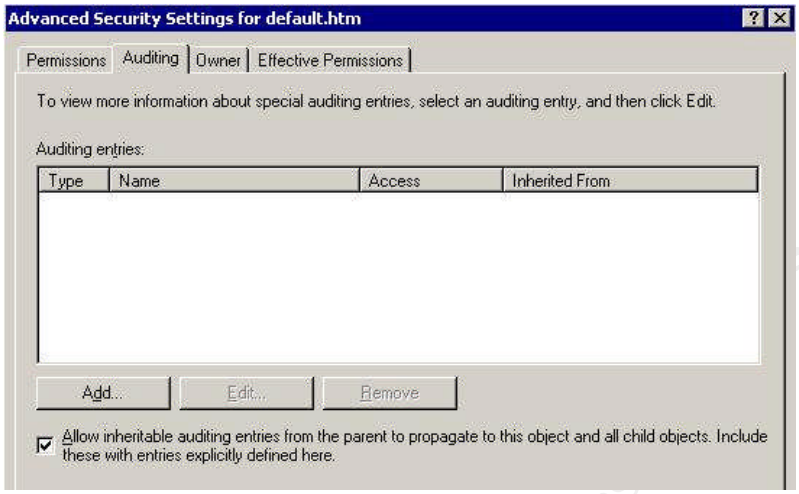
Audit object access – Success/Failure
For sensitive data, log failure and success. To enable audit object access, a System Access Control List (SACL) must be created, which is comprised of access control entries (ACE). An ACE consists of: [16]

1) A user, computer or group to be audited
2) Specific access type to be audited
3) A flag which indicated to audit failure, success, or both

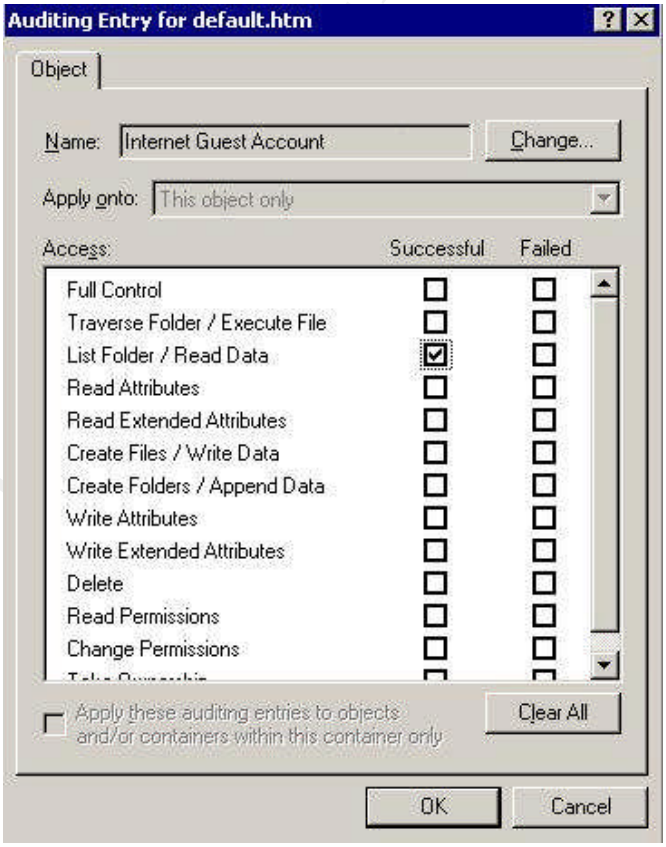
To audit access to a specific file

1) Browse to the file, right-click and select **Properties**
2) Select the **Security** tab, and then click **Advanced**

3) Select the **Auditing** Tab



4) Choose **Add…** and select the user to audit. In this example the Internet Guest Account (IUSR_*ComputerName*) is selected.



5) Choose which type of auditing is appropriate for the object. Auditing successful Read Data access on default.htm will likely yield many results, most of which is legitimate and to be expected. But the Internet Guest Account likely should not be writing to default.htm, so auditing

Write Data success may yield more relevant results.

Setting auditing on object access can overwhelm the system and decrease performance. Also, with too much information, it will be harder to find the more troublesome object access events amid all the normal audit events. For these reasons, keep object access auditing to a minimum and to only sensitive data and files.

Audit policy change – Success
Setting this option to log success will show policy changes on the server. This includes audit and user assignment polices.

Audit privilege use – Success/Failure
In a highly secure environment, logging both success and failure events will show all instances of when a user right is exercised. This includes bypass traverse checking, creating a token object, and the backup or restore of files and directories. However, due to excessive logging of privilege use events, logging only failure events will likely suffice. [16]

Audit system events – Success
System events are system shutdowns or events that affect system security. [14]

2) User Rights Assignment

There are many options available under User Rights, but we will only touch a few of the more important rights to assign. Other rights that can be assigned or denied include deny logon as service, debug programs, and deny log on through Terminal Services.

Allow log on locally – Administrators
Administrators should be the only group granted this right. By default, Account Operators, Backup Operators, Print Operators, and Power Users have this right as well, and should be removed.[18]

Deny access to this computer from the network – Guest, all NON-OS system service accounts, ANONYMOUS LOGON, SUPPORT_388945a0
This is a right that should be altered with care. This will prevent specified users from using SMB, NetBIOS, CIFS, HTTP, and COM+ over the network. This setting overrides the *Access this computer over the network*, in the same way a deny setting overrides any other rights. While the guest account is disabled, the group Guests includes the IUSR_*ComputerName* account, so don't deny access to the Guests group with this account still a member. [14]

Shut down the system – Administrator
Backup Operators and Power Users have this right on member servers by default.

3) Security Options

Below are some important and topical settings that apply to a web server and may need changed from the default setting. Others may apply depending on the environment, especially if the web server is a domain member and needs to contact domain controllers in a secure manner. The following settings are especially important to apply to a public facing web server.

Audit: Shut down system immediately if unable to log security audits – Enabled
This setting can cause significant server downtime. For sensitive data, if may be desirable to prohibit access if auditing fails. A system shutdown due to full event logs would require reviewing the server's event log size and overwrite settings.

Interactive logon: Do not display last user name – Enabled
This is especially useful if using Terminal Services to administer the machine remotely.

Interactive logon: Message text for users attempting to log on – Enabled
Interactive logon: Message title for users attempting to log on – Enabled
These two settings will present a warning message to users as they logon. While unlikely to deter an intruder, it should be enabled for legal reasons.

Interactive logon: Number of previous logons to cache – 0
This setting determines whether a user can logon with cached credentials if a domain controller is unavailable. Setting this value to 0 disables logon caching.

Interactive logon: Require Domain Controller authentication to unlock workstation – Enabled
Similar to disabling logon caching, this prevents an attacker from pulling a network cable from the server, and then logging on with old credentials.

Network access: Do not allow anonymous enumeration of SAM accounts and shares – Enabled
A popular method for fingerprinting servers, not allowing anonymous connections will help mask the server's identity.

Network access: Shares that can be accessed anonymously – none
Member servers allow access to COMCFG and DFS$ by default. Remove this access for improved security.

Network security: Do not store LAN Manager hash value on next password change – Enable
The LAN Manager hash is very weak, leaving system passwords more exposed than if this setting is disabled. After enabling this setting, administrators may have to change all passwords for the change to take effect. Also, test legacy or

third party applications that may depend on LAN Manger hashes for authentication. [16]

Conclusion

While far more secure than its predecessors, IIS and Windows 2003 require steps to harden the server against attacks. This paper addressed TCP/IP hardening, access controls, installation procedures, and which system services to disable.

Placement of the server behind a properly configured firewall is the first step to system security and a strategy of ongoing defense in-depth. And while not addressed here, patching is another critical security component. Patching for both the OS and IIS should be done in a reasonable time frame (a matter of days), as the time between patches and in-the-wild exploits is rapidly decreasing. Additional topics not covered here but also worth investigating for certain environments include authentication methods, application pooling, and SSL.

While every environment has different system requirements, this paper outlined a standard baseline of tighter IIS security from which upon others can build. For some installations, this guide will certainly be enough. But for other more complex deployments, topics like IPsec and advanced authentication methods may need to be investigated further.

References

1. Netcraft LTD. “April 2004 Web Server Survey” April 2004, http://news.netcraft.com/archives/web_server_survey.html

2. Belani, Rohyt and Muckin, Michael. “IIS 6.0 Security” March 5, 2004, http://www.securityfocus.com/infocus/1765

3. Binstock, Andrew. “What's new in IIS 6.0 and ASPs on Windows 2003 Server?” January 29, 2003, http://www.devx.com/SummitDays/Article/10648

4. Microsoft Corp. “Flaw in NetBIOS Could Lead to Information Disclosure (824105)” September 03, 2003, http://www.microsoft.com/technet/security/bulletin/MS03-034.mspx

5. Microsoft Corp. “Securing Internet Information Services 6.0” http://www.microsoft.com/smallbusiness/gtm/securityguidance/articles/sec_iis_6_0.mspx

6. Microsoft Corp. “HOW TO: Harden the TCP/IP Stack Against Denial of Service Attacks in Windows Server 2003” March 1. 2004, http://support.microsoft.com/default.aspx?scid=kb;en-us;324270

7. Sigma Solutions Corp. “Denial of Service Inhibitors” http://www.tcpiq.com/tcpiq/TcpipDOS/Default.asp

8. “Chapter 10 – Additional Registry Settings”. Threats and Countermeasures Guide. Microsoft Corp. http://www.microsoft.com/technet/Security/topics/hardsys/tcg/tcgch10.mspx

9. Szepesi, Dan. “What is Socket Pooling?” February 2, 2004, http://www.iis-resources.com/modules/wfsection/article.php?page=1&articleid=1

10. Microsoft Corp. “IIS 6.0: Setting Metabase Property DisableSocketPooling Has No Effect” January 12, 2004, http://support.microsoft.com/default.aspx?scid=kb;EN-US;813368

11. “Chapter 3 – Securing Web Sites and Applications”. Deploying Internet Information Services 6.0. Microsoft Corp. http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/all/deployguide/en-us/iisdg_sec_rmkz.asp

12. Binstock, Andrew. “What's new in IIS 6.0 and ASPs on Windows 2003 Server?” January 29, 2003, http://www.devx.com/SummitDays/Article/10648

13. Microsoft Corp. “Patch Available for 'Web Server Folder Traversal' Vulnerability” October 17, 2000, http://www.microsoft.com/technet/security/bulletin/MS00-078.mspx

14. Microsoft Corp. “Hardening Windows Server 2003 IIS Servers” http://www.microsoft.com/technet/security/guidance/secmod124.mspx

15. Shimonski, Robert J. “Locking Down IIS 6.0 with .NET: The Default Security Wizard” July, 18, 2002, http://www.windowsecurity.com/articles/Locking_Down_IIS_60_with_NET_The_Default_Security_wizard.html

16. Microsoft Corp. “Creating a Member Server Baseline for Windows Server 2003 Servers” http://www.microsoft.com/technet/security/guidance/secmod119.mspx

17. “Chapter 6 – Event Log”. Threats and Countermeasures Guide. Microsoft Corp. http://www.microsoft.com/technet/Security/topics/hardsys/tcg/tcgch06.mspx

18. Microsoft Corp. “Hardening Windows 2003 Bastion Hosts” http://www.microsoft.com/technet/security/guidance/secmod127.mspx