Global Information Assurance Certification Paper

Basic IIS 5.0 Default Web Server Security

Terri Carroll
GSEC (v.1.3)

Abstract / Summary:
Securing Internet Information Server 5.0 servers across a large corporation can be a complicated task when faced with many different scenarios and user set-ups. Whenever possible, it is best to set up a secure web site from scratch as it will be less complicated than trying to secure one that is already in use. Unfortunately, securing sites already in use is the challenge most administrators face.

Not every system will utilize all the features in IIS 5.0, but IIS, by default, makes most of its components available. Many of these components may not be needed for development (Example: FrontPage 2000 server extensions or sample pages and scripts), and can pose serious risks to the server. Though it is important to remember that no amount of hardening will make a system impenetrable, it should be stressed that taking a few extra steps will serve to help protect the systems. We will discuss some of those steps throughout this document. During the outbreak of the CodeRed Worm, I was on a client site that was using Windows NT 4.0 with IIS 2.0, 3.0 and 4.0. All the production servers successfully avoided being infected mainly because the system administrators had taken the time to configure the systems so that the worm was unable to infect them.

Assumptions:
The following assumptions are made throughout this document.

- All the systems discussed here are running a new installation (not an upgrade) of some flavor of Windows 2000 with a default installation of IIS 5.0. Web development is well underway; in fact a production system has already been placed on the Internet.
- Though the operating system (OS), Windows 2000, has been updated with all the appropriate service packs and hot fixes, the IIS servers have not been secured. You have been asked to secure the systems as quickly as possible.
- Your main focus is to secure the IIS Web Server application, not the OS or development code.
- You've backed up all the systems and are ready to begin.

First Step: Is IIS needed?
You just walked on to a new job and your first task is to help the web development group secure their development web servers as well as their

development system. There are three employees in the group, Joan, the group's administrative assistant, Bill the web developer, and Rachel the groups project manager. Upon examining all three systems you find they all have a default IIS installation. Do they all need it?

One of the first steps in securing a web server is understanding its usage. If you are not careful it is easy to "break" the functionality of an already existing system. You must talk with the developers and determine the services and applications needed, and understand the purpose of the site. For the purpose of this document, it is determined through discussions with the group that Joan, the administrative assistant, doesn't use her installation of IIS. However, Bill and Rachel use their installations on a daily basis.

If the IIS server is unneeded as is the case with Joan, the single best way to secure the box is to un-install IIS. Some default installations of Windows 2000 include IIS. It is amazing how many users have IIS installed and don't even know it is running on their systems. I mentioned earlier that while on a client site the production systems avoided infection from CodeRed. I want to now continue that example by stating that at the same client site numerous infections were found on internal systems. Most of those infections were on employee workstations and most of them didn't even know IIS was running. So, for the first step, remove IIS from systems that do not require it.

To un-install IIS 5.0 from a default Windows 2000 installation, follow these steps:

1. Click the [Start] Button, choose "Settings", and select "Control Panel".
2. Open the "Add/Remove Programs" Icon
3. Select the "Add/Remove Windows Components" option.
4. Uncheck the box next to the "Internet Information Services (IIS)" option and click the [Next>] button.
5. The Microsoft Windows Components Wizard will complete the un-install.
6. When the un-install is complete, click the [Finish] button to close the Wizard.
7. Click the [Close] button to close the "Add/Remove Programs" box.
8. Close the Control Panel Window.
9. The Internet Information Service (IIS) has been removed.

NOTE: If you realize later that IIS is needed, the Windows installation CD may be needed to complete the re-installation.

Second Step: Update the IIS Application

Both Bill and Rachel have indicated that they use their IIS servers everyday. In

fact, the system Rachel is in charge of is the production system that serves pages to the Internet. In addition to the OS patches and hot fixes, Microsoft releases patches and hot fixes for their individual applications as well, including IIS. On April 10, 2002, Microsoft released a cumulative patch for Internet Information Server. This hot fix included all the patches and hot fixes specific to IIS up until the day of release and is one of the fastest way to get the application up to date when accompanied by any other hot fixes released following that patch. For more information about this patch visit: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-018.asp . Another way to get your application up to date, especially if you don't know what patches have already been installed, is to use the HFCheck tool, released by Microsoft. It will help get you up and keep you up-to-date. For more information on this tool or to download it, visit: http://www.microsoft.com/Downloads/Release.asp?ReleaseID=24168. Microsoft patches are an essential part of keeping your systems secure. However, it should be noted that in some companies for whatever reason, the use of Microsoft patches is not always a standard policy or immediately allowed. That is why it is so important to know other ways of securing the systems. For more information on security bulletins and patch information visit Microsoft's Security Bulletin web site at: http://www.microsoft.com/technet/security/current.asp

Third Step: Default IIS Installations: Is Everything Needed?

Once the patches are installed, the next step is similar to that of the first. What is needed? What is not? The default installation of IIS installs four different servers: NNTP, SMTP, FTP and WWW. What are they? What are they used for? And do you need them? Answering these questions and removing what is not needed is your next step. Below is a description of each of the servers. Determining their need will depend on the policy of your company and purpose of your web server.

NNTP Server:

NNTP stands for Network News Transfer Protocol and uses TCP port 119 to transfer articles between news servers and can also be used to read and post articles. NNTP is one of the most commonly scanned ports and if found to be vulnerable, it will be exploited.

SMTP Server:

SMTP stands for Simple Mail Transfer Protocol. SMTP utilizes port 25 to transport mail across the Internet. Like NNTP, the SMTP server is susceptible to various security vulnerabilities.

FTP Server:

FTP stands for File Transfer Protocol and uses TCP ports 20 and 21 to exchange files over the Internet. It is a very common and widely used protocol. Though many web servers will not utilize NNTP or SMTP it is very possible they will use FTP. However, like the other protocols if it isn't being used, it shouldn't be installed. FTP is also commonly scanned for vulnerabilities and will be targeted if not secured.

WWW Server:

The most widely used IIS server is the WWW Server. WWW stands for World Wide Web. The WWW Server uses the Hypertext Transfer Protocol (HTTP) over port 80 to serve up web pages to the Internet. HTTP combined with //: introduces a Uniform Resource Locator (URL) usually referred to as a Web address. (Example: http://www.sans.org.) If you want the IIS server to serve web pages to the Internet or Intranet, you will need this service. Since your web server won't run without it, is it very important to make this component of IIS as secure as possible. This service is also susceptible to many various attacks. Though perhaps not successful, it is likely that every IIS web server on the Internet was attacked, at one time or another, by either or both the CodeRed and/or Nimda Worms.

It is important to understand and determine the need for these types of servers since each has been targeted at one time or another. Please note that whether or not a specific "attack" mentioned here targets your particular set up, it is important to remember that even if you are not vulnerable to this attack, you might be vulnerable to the next. It is best to remove all unneeded services, servers, and protocols whether or not they are considered vulnerable today.

Bill only uses his IIS Server for Web page development and Rachel merely monitors the production version of his development server. Therefore we will eliminate the NNTP, SMTP, and FTP servers. What other components might the users not need? Is the user developing their web pages with Microsoft FrontPage? If not, the FrontPage 2000 Server Extensions component should be removed. Do they use the Documentation installed with IIS? What about the Internet Services Manager (HTML)? It may seem overly cautious to remove everything that is not being used, but remember that the less components, applications, and services running on the system, the less possible vulnerabilities and entry points an intruder may some day find. To remove all the unneeded components:

1. Click the [Start] Button, choose "Settings", and select "Control Panel".
2. Open the "Add/Remove Programs" Icon
3. Select the "Add/Remove Windows Components" option.

4. Highlight the “Internet Information Services (IIS)” option and click the [Details…] button.
5. Uncheck the box next to any IIS component that the user/application does not need.
    a. SMTP
    b. FTP
    c. NNTP
    d. Documentation
    e. FrontPage 2000 Server Extensions
    f. Internet Service Manager (HTML) – Web Interface
    g. Visual InterDev RAD Remote Development Support (This will be removed automatically if you remove the FrontPage server extensions.)
6. Click the [OK] button to continue.
7. Click the [Next>] button to continue.
8. The Microsoft Windows Components Wizard will complete the un-install of the selected components.
9. When the un-install completes, click the [Finish] button to close the Wizard.
10. Click the [Close] button to close the “Add/Remove Programs” box.
11. Close the Control Panel Window.
12. The selected Internet Information Service (IIS) components have been removed.

Fourth Step: Securing the Default Web Site

The idea of “Best Practice” would advise that the “Default Web Site” be deleted and a new one created before deploying the site. Unfortunately in the “real world” it is often the case that this luxury is not available within the “policies” of a company. Whatever the case, administrators are often faced with having to secure the “Default Web Site.” Such is the case in our scenario where the system administrator has been called upon to secure a web server already in use that was not set up using the concept of “Best Practice.”

Once you have determined which servers and which components are necessary you can begin taking further manual steps to help ensure the security of the web server. Bill and Rachel will only be using the web server (WWW), therefore the other servers and components discussed above have been removed. However, the following changes to the default IIS installation should be made even if you keep some of the other components.

<u>Deleting the Un-needed Directories</u>

Before deleting, removing or renaming any directories, always confer with your web developers. Understand the usage of the system before assuming whether

or not the changes you are about to make will affect the site.

In our example, we have backed up all the systems and are making changes to Bill's development server before making any changes to Rachel's production server. By doing so, we can check for problems before implementing the changes on the production system. Then, assuming the systems are identical, we can make the same changes on the production server. Using the steps below, remove the listed directories if they exist on the hard drive.

1. Click the [Start] Button
2. Choose "Programs"
3. Choose "Accessories" and select "Windows Explorer"
4. Expand the "My Computer" link by clicking the "+" beside the option.
5. Expand the "Local Disk (C:) link by clicking the "+" beside the option.
6. Continue to Navigate to each of the directories listed below in the same manner.
7. When a desired directory is found, right click on the folder you wish to delete.
8. Select the "delete" option from the menu.
9. Confirm the operation.
10. Repeat for each folder below.

    - C:\inetpub\iissamples
    - C:\inetpub\AdminScripts
    - C:\WINNT\help\iishelp
    - C:\WINNT\system32\inetsrv\iisadmpwd
    - C:\WINNT\web\printers

Since, in our example, none of our users are using SMTP or NNTP we can also delete the following directories if they exist on the hard drive:

- C:\Inetpub\mailroot
- C:\Inetpub\nntpfile
- C:\WINNT\Help\mail
- C:\WINNT\Help\news

Edit Master Properties

If you set the properties of an individual web site, the "Default Web Site" for instance, rather than to the master properties, any new sites will inherit the default (unsecured) settings. So instead, we will edit the master properties for the server, which will keep the server more secure, by replicating the same more secure standards on any new web sites created.

To Get to the Master Properties:

1. Click the [Start] Button
2. Choose “Programs”
3. Choose “Administrative Tools” and select “Internet Service Manager”
4. Right click on the server and select the “Properties” option
5. You will see two tabs: **Internet Information Services** and **Server Extensions**.
6. Under the **Internet Information Services** Tab, select the “WWW Service” listed in the drop down box under “Master Properties:” and click the [Edit] button.
7. A box with several more tabs appears.

NOTE: If at anytime during these steps you see the “Inheritance Overrides” properties box, click the [Select All] button and then click the [OK] button to continue.

Within the Master Properties we will complete the following changes:

- Enable logging
  Enabling logging will allow you to monitor the usage of your web site as well as to investigate any actual or potential attack.

  From step number 7 above:

  8. Confirm that the check box next to “Enable Logging” is selected and that under the “Active Log Format” drop down box the “W3C Extended Log File Format” is chosen.
  9. Click the [Properties] button
  10. Under the Extended Properties tab verify that there is a check mark next to the following options. **NOTE**: Some of these are checked by default, some will need to be added.

Client IP Address	HTTP Status	Server Port
User Name	Win32 Status	Cookies
Method	User Agent	Referrer
URI Stem	Server IP Address	

  11. Click the [OK] button to close the “Extended Logging Properties” page.

- Remove Unnecessary Application Mappings
  Removing unused application mappings removes potential vulnerabilities. This was the case in the example I gave earlier about the administrator who

avoided the CodeRed worm. Along with some other security steps, he also made sure to remove unneeded application mappings, including the .ida and .idq mapping exploited by CodeRed.

When deleting, removing, or renaming you should always discuss what you are doing with your developer to be sure you will not take away functionality of the web server.

From step number 7 above:

8. Select the **Home Directory** Tab.
9. Click the [Configuration…] button.
10. Under the **App Mappings** Tab, in the "Application Mappings" box, highlight the mapping to be deleted and click the [Remove] button.
11. Delete the following application mappings.

.asa	.cer	.idc	.shtm
.asp	.htr	.idq	.shtm
.bat	.htw	.print	l
.cdx	.ida	er	.stm

- **NOTES**:
  - The extensions .asa and .asp are very commonly used and should be remove with caution.
  - Not all these mappings are part of the default install, therefore they may not be present in your installation, but you should check for them just the same.
  - This step may very well remove all your app mappings; this is not a problem for functionality as long as none of the associated applications are in use. (Did you talk with your developer?)
  - Use of the Add/Remove program may cause the mappings to return to default. Use caution and check the app mappings if you use the Add/Remove program.

- Disable the Parent Paths
  According to Michael Howard in his document entitled, "Secure Internet Information Services 5 Checklist," this option allows users to use ".." in calls to functions such as MapPath, and it should be disabled.

  After removing the application mappings, to disable the Parent Path from step number 11 above:

  12. Select the **App Options** tab.

13. Remove the check mark next to the “Enable parent paths” option.

- Use Text Error messages
  By default IIS 5.0 sends a detailed ASP error message to the client when an error occurs on the page. While this is desirable during development, since having as much information about the error assists in fixing it, this may not be so desirable in production. The potential that the detailed page will give too much “detail” to a potential hacker is such that it is recommended that a carefully worded custom text message should be used instead.

  After disabling the Parent Path, follow these instructions from step 13 to use text error messages.

  14. Select the App Debugging tab.
  15. Check the “Send text error message to client” option.
  16. Modify the text to read whatever is appropriate for your site, or use the default text provided.
  17. Click the [OK] button to exit the “Home Directory/Configuration” utility.
  18. Click the [OK] button to exit the “WWW Service Master Properties” page.
  19. Click the [OK] button to exit the Server “Properties” page.

  In our example, Bill is the developer and may need this information; we will leave this option on his system. However, on the production system overseen by Rachel we will remove this option so that the general public does not see the details when and if an error occurs.

Delete the IIS “Default Web Site” Directories from the Application

Ideally the default web site would be deleted. Then a new site would be created using directory and folder names that are not obvious to the user of the site (no default or obvious names). This would eliminate the need for this step; however, since it is fairly common that web site creators use default set-ups it is important to understand how to remove the directories, which may be vulnerable.

By completing the section on removing directories from the hard drive (the first step in this section), we have effectively removed some of the directories we will discuss here; a red error icon may indicate them. Following will be a list of directories that should be removed, but it should be noted that ANY directory not in use, should be removed.

In addition, it should be recommended to the developer that any files in use in default directories should be moved to new directories or, at the very least, the directory name should be changed. Additionally, if not already done, the “Default Web Site” should also be renamed. **NOTE:** This may require code

changes so don't expect the established web developer to complete this recommendation immediately, but emphasize its importance.

Within the Internet Information Service Manager (IIS Manager) delete the following directories if they exist and are not in use under the "Default Web Site."

To remove these directories from the Internet Information Services Manager:

1. Click the [Start] Button, choose "Programs"
2. Choose "Administrative Tools" and select "Internet Services Manager"
3. Expand the server link by clicking the "+" beside the server name.
4. Expand the "Default Web Server" by clicking the "+" beside it.
5. By default the following directories should exist. Delete all that are not in use. If there are directories other than the one's listed, discuss them with your developer to determine if they can be deleted as well.

   a.
   b. Scripts
   c. IISHelp
   d. IISAdmin
   e. IISSamples
   f. MSADC
   g. Printers
   h. Images
   i. _private
   j. _vti_cnf
   k. _vti_log
   l. _vti_pvt
   m. _vti_script
   n.

6. Right click on the directory to be deleted.
7. Select the "Delete" option from the menu.
   NOTE: In some cases, this step will delete actual directories off the hard drive; in other cases it will merely delete a link or virtual directory. If you are sure the linked directory is not needed, you should delete the actual associated directory as well.
8. Confirm the deletion.
9. Close the Internet Information Services window.

Step Five: Access Control Lists (ACLs)

We have secured a great deal of the application by eliminating possible physical vulnerabilities. Let's take a look now at who has access to what. Many of the files and directories give access to "Everyone" by default. In many cases, this is like an invitation to a hacker, so let's remove this invitation.

ACLs need to be set both at the base Operating System level as well as within the IIS server itself. As indicated by Microsoft documents, "From Blueprint to Fortress: A Guide to Securing IIS 5.0" by John Davis and "Secure Internet Information Services 5 Checklist," by Michael Howard, it is suggested that the ACLs for particular file types should be set as follows.

For CGI (.exe, .dll, .cmd, .pl)
- Everyone (executable)
- Administrator (full Control)
- System (Full Control)

Include Files (.inc, .shtm, .shtml)
- Everyone (executable)
- Administrator (Full Control)
- System (Full Control)

Script Files (.asp)
- Everyone (executable)
- Administrator (full Control)
- System (Full Control)

Static Content (.txt, .gif, .jpg, .html)
- Everyone (read-only)
- Administrator (Full Control)
- System (Full Control)

NOTE: Never install executable files in the same directory as your web content. Remember that the *Write* and *Execute* IIS permissions should NEVER be assigned to any folder accessible to anonymous users.

For Example:
On Bill's system, lets assume the following: We have deleted unneeded directories from the hard drive and from the default web server. However he is using the following default directories, scripts and images. In addition, his root directory contains his home .html page. We have recommended that he rename the directories, change his code and rearrange the placement of his files so that files of similar type are together. However, in the meantime we need to secure what is left.

In this case, the Script directory will have ACLs set to Everyone (execute), Administrator (Full) and System (Full) where as the home directory and the images folders will give Everyone (read-only) access, Administrators and System (Full Control).

Be sure to check the ACLs on the physical directory as well as on the directories in IIS.

In fact, one other recommended ACL change from Michael Howard's document, "Secure Internet Information Services 5 Checklist," is for the log file directory at C:\WINNT\System32\logfiles. It is recommended the ACLs be set to Administrators (Full Control), System (Full Control), Everyone (RWC) thus helping to keep hackers from attempting to cover up their tracks.

Conclusion:
Using IIS to create web sites is a very popular process. It provides a convenient graphical user interface and practically sets up the server for you. However, this convenience does not come without a cost. Best practice would dictate the development of a new server rather than use of the default server, because of

default vulnerabilities. However, though the risks are becoming better known, many web developers and home users are unaware of the risks associated with a default set up, and as a result continue to use it for convenience.

This document does not cover the steps to create the most secure IIS web server, and does not cover all the steps that could be used; using the Hisecweb.inf security template, emphasizing the use of a partition separate from the OS for your IIS document root, or making specific registry changes, for example. To that end, it is not meant to replace the steps of creating a "Secure" server, but rather it strives to give the users of the convenient "Default Server", some ways to protect themselves until they can put together a properly secured system.

This document does cover some very good steps. The steps outlined here were enough to have protected many systems from the outbreak of the CodeRed worm and may have assisted in preventing spread of the Nimda worm, which were two of the most wide spread worms to have affected IIS systems.

If you have the ability, time, and luxury to create an IIS server from the ground up, many of the documents listed in the reference section provide more detailed information and should be consulted.

Any system connected to the Internet has the potential for exploit no matter how "secure" we think it is. As administrators of web servers, at home or in the office, we have the responsibility to secure the systems as best we can within the guidelines of our company's security policies or by defining the amount of risk we are willing to take with our systems and the information on them.

References:

"Microsoft Security Bulletin MS01-043 - NNTP Service Contains Memory Leak." August 14, 2001, Revised V1.1 August 15, 2001. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms01-043.asp (March 28, 2002)

"Microsoft Security Bulletin MS02-011- Authentication Flaw Could Allow Unauthorized Users To Authenticate To SMTP Service." February 27, 2002, revised V2.0 March 12, 2002. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-011.asp (March 28, 2002)

"Microsoft Security Bulletin MS01-044 - 15 August 2001 Cumulative Patch for IIS." Originally posted: 15 August 2001, V1.1 August 20, 2001, URL:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-044.asp (March 28, 2002)

Davis, John, Microsoft Corporation, "From Blueprint to Fortress: A Guide to Securing IIS 5.0". Published: June 2001, Microsoft Word Document. URL: http://www.microsoft.com/serviceproviders/whitepapers/securing_iis_whpaper.doc (March 29, 2002)

The University of North Carolina at Chapel Hill, ITS Security at UNC – Chapel Hill "Securing IIS 5.0," last modified: 27 November 2001, URL: http://www.unc.edu/security/securing_iis.html (March 29, 2002)

Howard, Michael. Microsoft. "Secure Internet Information Services 5 Checklist." 29-June-2000. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/iis/tips/iis5chk.asp (March 29, 2002)

SecurityFocus, "Securing IIS 5.0." Last updated, Fri Aug 24 2001. URL: http://online.securityfocus.com/infocus/1312 (March 29, 2002)

Whiteside, Dawn. "Securing IIS: Checklists." Adapted from Jason Fosse's course 'Securing IIS 5.0', SANS Institute. Last Modified 09-Oct-2001 URL: http://ist.uwaterloo.ca/~dwhitesi/docs/IIS/checklist.html

Courington, David S. "A Step-by-Step Guide to Securing Windows 2000 for Use as an Internet Server." March 29, 2001. URL: http://rr.sans.org/win2000/win2000_sec.php (March 29, 2002)

Symantec. "W32.Nimda.A@mm." Discovered on: September 18, 2001, Last Updated on: December 13, 2001 at 04:41:06 PM PST URL: http://securityresponse.symantec.com/avcenter/venc/data/w32.nimda.a@mm.html (April 8, 2002)

Symantec. "CodeRed Worm." Discovered on: July 16, 2001. Last Updated on: September 19, 2001 at 10:26:21 AM PDT URL: http://securityresponse.symantec.com/avcenter/venc/data/codered.worm.html (April 8, 2002)

ITC - UVa Information Technology and Communication, "The Ten Most Critical Internet Security Threats." Last updated: Tuesday October 2, 2001, URL: http://www.itc.virginia.edu/desktop/security/local_summary.html (April 9, 2002)

Figueroa, Michael A. - The AMS Center for Advanced Technologies.

"Technology Brief - Protecting IIS 5.0 Web Servers." Volume 1, Number 9, December 2001. PDF: URL: http://www.ams.com/Amscat/Downloads/ProtectingIIS.pdf (April 11, 2002)

"Microsoft Security Bulletin MS02-018 - Cumulative Patch for Internet Information Services (Q319733)." V1.0 April 10, 2002, V1.1 (April 11, 2002): URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-018.asp (April 11, 2002)