Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Securing Microsoft's Internet Information Server 5.0

Internet Information Server (IIS) 5 is Microsoft's premier web server product and is fully integrated into the Windows 2000 operating system. It supports many of the latest Internet standards for creating and sharing web based applications. This paper will provide IIS administrators with the steps to secure their web server installations. Please note that although this paper deals with Windows 2000 and IIS 5 some of the following guidelines can be applied to older versions of those products.

Copyright SANS Institute

Author Retains Full Rights

AD

Securing Microsoft's Internet Information Server 5.0
Ben White
Version 1.2e
August 31 2001

Introduction

Internet Information Server (IIS) 5 is Microsoft's premier web server product and is fully integrated into the Windows 2000 operating system. It supports many of the latest Internet standards for creating and sharing web based applications. This paper will provide IIS administrators with the steps to secure their web server installations. Please note that although this paper deals with Windows 2000 and IIS 5 some of the following guidelines can be applied to older versions of those products.

Securing Windows 2000

The first step to a secure IIS sever is to secure the base operating system itself.
As stated in Hardening Windows 2000 by Philip Cox "The best way to secure a system is to use it for one purpose and secure it around that specific purpose. This should be your goal: one service, one system."[1]To that end, finding and disabling all unneeded services and network protocols should be a priority. The following list of services, taken from Hardening Windows 2000 by Philip Cox, are the minimum required to run a Windows 2000 standalone server. This list can be used as a base from which to build.

- DNS Client
- Event Log
- Logical Disk Manager
- Plug & Play
- Protected Storage
- Security Accounts Manager
- Server
- Workstation[2]

If SMTP (mail) or NNTP (news) services are not installed and the server is not part of a domain, then the Server and Workstation services can also be disabled. Contrary to popular belief these services are not needed in order for IIS to function. To disable a service open Control Panel | Administrative Tools | Services. Double click the service you wish to disable and on the service's properties sheet change the Startup Type field to Disabled. You can then either stop the service if it's already running or reboot the server for the changes to take effect.

[1] Cox, p. 1

[2] Cox, p. 6

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

It's highly recommended that you setup your web server as a standalone or workgroup server using only TCP/IP as your networking protocol. One of the biggest security risk with the Windows operating system is NetBIOS, so be sure to disable NetBIOS support or block TCP /UDP ports 135 thru 139 at your network border. New to Windows 2000 is TCP port 445, which allows the running of SMB over TCP, and should also be blocked at your network Border.

To disable NetBIOS at the host open Control Panel | Network and Dial-up Connections. Right click the connection and choose Properties from the context menu. Highlight Internet Protocol (TCP/IP) and again choose Properties. Once the Properties box opens choose Advance | WINS and select Disable NetBIOS over TCP/IP. Disabling File and Print sharing for Microsoft networks will also accomplish the same task. To do so, open Control Panel | Network and Dial-up Connections. Right click the Connection and choose Properties from the context menu. On the connection's property box, deselect File and Print Sharing for Microsoft Networks.

Alternately Windows 2000 IPSec can be used to block unnecessary protocols and ports. IPSec (Internet Protocol Security) provides authentication services for IP traffic. The IPSec interface in Windows 2000 provides that as well as other network access protections for the Windows 2000 operating system. I highly recommend using IPSec to provide another layer of defense for your web server installation.

Lets walk thru building a custom IPsec policy to block access to port 23 on the web server. For a standalone Windows 2000 server we'll use the Local Security Policy applet found in Control Panel | Administrative Tools. After opening the Local Security Policy, applet highlight IP Security Polices on Local Machine then right click and choose Create IP Security Policy from the context menu. This will start the IP Security Policy Wizard. Click Next to proceed to the second page and name the policy "Telnet". Click Next and on the third page clear the Activate the default response rule box. Click Next again, make sure that the Edit properties box is checked, and click Finished.

At this point the New IP Security Policy properties box will appear. Make sure that the Use Add Wizard box is checked and click Add. This will open the Security Rule Wizard click Next to proceed to the second page. Accept the default selection (This rule does not specify a tunnel) and click Next. Again accept the default selection (All network connections) and click Next. On the Authentication Method page select Use this string to protect the key exchange then type in any string that you wish. For example, you might choose to use the string "securewebserver". Please note, however, that you can't use a blank string. Click Next to move to the IP filter List page then click Add. This is where we'll build the list of protocols and ports this policy rule will apply to.

Name the IP filter list "Port 23" and click Add. This will open the IP Filter Wizard click Next to proceed. On the IP Traffic Source page accept the default (my IP address) and click Next. On the IP Traffic Designation page accept the default (any IP address) and click Next. On the IP Protocol Type page select the TCP protocol for this filter from the drop down menu and then click Next. On the IP Port page you can select the option From

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

This Port to select a source port or choose the option To This Port to select a designation port. If you don't choose a specific port the rule will apply to all ports for the chosen protocol. In this case we'll choose "from this port" and type "23" in the field for the source port and leave the default "to any port" for the designation. This rule will govern how TCP traffic between port 23 of the web server and any port on any remote computer is handled. Click Next and then Finished to close the window and save the settings. You will now see displayed at the bottom of IP filter Wizard a summary of the IP filter you just created. You're free to add more protocols and ports to the list by clicking the Add button again. When finished, clicking Close will bring you back to the Filter List page.

Now choose the filter you just created "Port 23" and click Next. Our next task will be to choose the action to apply to this rule. You can choose from the list or click Add to create a new action. Clicking Add opens the Filter Action Wizard click Next to proceed. On the Filter Action Name page type in "Block" and click Next. On the Filter Action General Options page the actions Permit, Block, and Negotiate Security are listed. Since we'll need to block access go ahead and choose the option "block". As before click Next and then Finished to close the wizard and save the settings. Now choose the action you created and click Next. If you wish to go over your settings leave the Edit box checked, otherwise clear this box and click Finished. Click Close to exit the new Policies property box. The last step is to right click the newly created policy "Telnet" and choose Assign from the context menu. With this policy enabled the webserver will reject any connection attempt to port 23. If at any time you wish to disable the policy simply right click it and choose un-assign from the context menu.

The following list displays some common IP ports and services.

PORT	SERVICE	DESCRIPTION
20 TCP	FTP	FTP Data
21 TCP	FTP	FTP Control
23 TCP	Telnet	Telnet
25 TCP	SMTP	Simple Mail Transfer Protocol
53 UDP	DNS	Domain Name Service Lookup
80 TCP	HTTP	HyperText Transfer Protocol
110 TCP	POP3	Pots Office Protocol Version 3
119 TCP	NNTP	Network News Transfer Protocol
443 TCP	HTTPS	Secure HyperText Transfer Protocol

A complete listing can be found at this URL

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

http://www.xploiter.com/security/ports.html

Our next stop is System Policy. Though a detailed discussion of System Policy is beyond the scope of this paper. There are still a few tools that we should consider, which can make the job easier.

The Windows 2000 Internet Server Security Configuration Tool for Internet Information Server 5 (IIS5) enables IIS administrators to configure many aspects of the Windows 2000 Operating system and IIS. Instructions for using this tool are included with the download. It's available at this URL

http://www.microsoft.com/Downloads/Release.asp?ReleaseID=19889

In addition to this tool Windows 2000 provides the Security Configuration and Analysis MMC snap-in. This tool allows you to open security templates, analyze the current configuration against those templates, and then change your current configuration based on any differences between them. The templates, which are located in %systemroot%/Security/Templates, provide system policy settings for many different server configurations. Microsoft also provides a new security template for servers running IIS5. The template called Hisecweb.inf is available at this URL

http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/iis/tips/iis5chk.asp

The following steps for using the template where taken from Secure Internet Information Services 5 Checklist by Michael Howard:

- Copy the template to the %windir%\security\templates directory.
- Open the Security Templates snap-in, and look over the settings.
- Open the Security Configuration And Analysis snap-in, and load the template.
- Right click the Security Configuration And Analysis snap-in, and choose Analyze Computer Now from the context menu.
- Wait for the work to complete.
- Review the findings and update the template as necessary.
- Once your happy with the template, right click the Security Configuration And Analysis snap-in and choose Configure Computer Now from the context menu.[3]

For additional help with using the Security Configuration and Analysis snap-in see its help files.

---

[3]Howard, p. 2

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Finally to close out the section on Securing Windows 2000, I'll list some additional steps that you should implement.

- Apply the most recent Service pack and Hotfixes.
- Use NTFS partitions.
- Remove the Everyone group from all NTFS directory and file permissions list.
- Review NTFS permissions and group memberships for all user accounts. Use the most restrictive permissions where possible.
- Remove the SAM file from the WINNT/REPAIR directory.
- Create the users group TelnetClients. Once this group is created only it's members will be allowed to use Telnet to access the server. Also the Telnet server for Windows 2000 can be set to use NTLM authentication only. See Microsoft Knowledge Base article [Q253918] for more details.
- Disable the POSIX and OS/2 subsystems by deleting their strings from the value "Optional" found in the Registry entry: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SessionManager\Subsystems.

Securing Internet Information Server

Now lets take a look at some IIS 5 installation issues. First, if you're upgrading from an earlier version, uninstall that version before upgrading. This will prevent any vulnerability from the old installation migrating to the new. Next install only the server components you need. One component I strongly suggest you don't install is FrontPage Server Extensions. Front Page Server Extensions can be used to manage a web site remotely. It's strongly recommended that when possible you choose to manage your web site locally. If you install the FTP and SMTP components the following two directories will be created.

- C:\inetpub\ftproot
- C:\inetpub\mailroot

You should place the directories on a volume other than the one that holds the IIS server's webroot directory and be sure to remove the group Everyone from the NTFS permissions list. In most cases the FTP server will be setup as an anonymous server. Please note that if the FTP server is configured to use Windows 2000 user names and passwords that those credentials will be passed in clear text over the network.

The IUSR_*computername* account is created during installation to provide anonymous access to your web site. You're free to use any user account you wish for anonymous access, but make sure to grant the account the user right to "log on locally" and to set your NTFS permissions accordingly. To change the anonymous user for IIS, first open Control panel | Administrative Tools | Internet Service Manager. Right click the server and choose Properties from the context menu. From the master properties of the WWW

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

service click Edit. On the Master Properties box click the Directory Security tab and then click Edit for the property Anonymous Access and Authentication Control. On the Authentication Methods property box once again click Edit to change the account name for Anonymous Access.

Once your web server components have been installed the next step is to check that there are no sample applications installed. You should never install samples on a production server. The following list[4], taken from Securing Internet Information Services 5 Checklist by Michael Howard, shows the locations for some of the samples you'll want to remove.

Sample	**Virtual Directory**	**Location**
IIS Samples	\IISSamples	c:\inetpub\iissamples
IIS Documentation	\ISSHelp	c:\inetpub\help\iishelp
Data Access	\MSADC	c:\program files\commonfiles\system\msadc

To remove the samples, delete both the application package and the actual directory. To delete the application package, open Control Panel | Administrative tools | Internet Services Manager and double click your web server. The application packages will be listed under the Default and Administration web sites installed with IIS 5. Please note you can group applications and other file types by directory and then control access thru NTFS permissions on those directories. Files would be setup to inherit permissions from their parent directory. For example, you might place all your asp files in the directory d:\websever\asp and then give the user account IUSR_*computername* the NTFS permission "Read and Execute" for that directory. I would also recommend that for any directory that holds ASP scripts, CGI applications or ISAPI applications that you disable the IIS Read right. By default all files are assigned IIS read rights. With Read access enabled users can download the application instead of executing it. Please note the directory must still include the NTFS Read permission. To disable IIS Read access for a web site open Control Panel | Administrative Tools | Internet Services Manager. Right click the web site and choose Properties from the context menu. The option to enable or disable Read or Write access is found on the Home Directory page.

The next step is to remove unused script mappings. These mappings are used to support filename extensions such as .asp. The following, taken from Securing Internet Information Services 5 Checklist by Michael Howard, is a list[5]of mappings to remove if they're not needed.

[4] Howard, p. 6

[5] Howard. p. 6

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

If you don't use….	Remove this entry:
Web-based password reset	.htr
Internet Database Connector	.idc
Server-side Includes	.stm, .shtm and .shtml
Internet Printing	.printer
Index Server	.htw, .ida and .idq

To remove a mapping open Control Panel | Administrative Tools | Internet Services Manager, right click the web server and choose Properties from the context menu. From the Master Properties of the WWW service click Edit. Click the Home Directories tab and choose Configuration. On the Apps mapping page choose the mapping and click Remove. You'll be prompted if you want the change to be inherited by certain child modules of the main WWW service. Look over the modules listed and click OK to apply the change to them also.

The next step is to disable the Parent Paths option. Parent Paths allows you to use such options as the "File" keyword with the syntax "..\" to include a file from a parent directory. This option could be used to browse outside the web root directory. To disable the option, open Control Panel | Administrative Tools | Internet Service Manager, right click the web site and choose Properties from the context menu. Next click the Home Directory tab and click Configuration. Now click the App Options tab and clear the Enable Parent Paths check box.

If you don't want users to be able to browse the folder contents of your web site then you should disable Directory Browsing. To do so, open Control Panel | Administrative Tools | Internet Service Manager, right click the web site and choose Properties from the context menu. Click the Home Directory tab and clear the Directory Browsing check box.

Next check your web root directory for files not related to the content of your site. Programs used during the construction of the site may have created many temporary and backup files. The extensions used by these files are not mapped by IIS, therefore a user may be able to view the file's contents. For example, a backup of an IDC file could contain user credentials to a backend database. Also be sure your web root directory is not on the volume that contains your system files.

If you're using Network Address Translation or NAT to hid your web server's internal IP address. You should disable the ability of the Content-Location header from exposing the Web server's IP address. To do so, open a command prompt and change to the directory c:\inetpub\adminscripts, then type "adsutil set w3svc/UseHostName True". Note you may be prompted to change your default script engine before the command will execute. Reboot the server for the change to take effect. When done the Content-Location header will display the Fully Qualified Domain Name of the server instead of the internal IP address. For more information see Microsoft Knowledge Base article [Q218180].

Next you'll want to enable logging for your web site. To do so, open Control Panel | Administrative Tools | Internet Service Manager, right click the web site and choose

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Properties from the context menu. Click the Web site tab and check the Enable Logging check box. Choose W3C Extended Log File Format from the Active Log Format drop down menu. Click Properties and then click the Extended Properties tab to set the log properties. The following, taken from Securing Internet Information Services 5 Checklist by Michael Howard, is a list of properties you should set.

- Client IP Address
- User Name
- Method
- URI Stem
- HTTP Status
- Win32 Status
- User Agent
- Server IP Address
- Server Port[6]

To prevent the log files from being altered make sure the NTFS permissions for the log file folder, located at %systemroot%\system32\logfiles, are set to Full Control for Administrators and Full Control for SYSTEM.

Third Party Security Tools

There are just three categories that I think are worth mentioning, Integrity checking software, Intrusion Detection Systems and network sniffers.

Integrity checking software works by taking a "snapshot" of your system's files. The snapshot will contain information on many of a files attributes, it will also contain a Cyclic Redundancy Check and Hash. You would take the snapshot right after you have finished building your system, then place that snapshot on CD-Rom to prevent tampering. At any time the snapshot can be compared against the current state of the system to determine if any files have been changed or corrupted. This can help you spot Trojan horse programs and hacker rootkits. I highly recommend that you think about using such software on your web server.

A host based Intrusion Detection System or IDS can help you spot and track hacking attempts. These products will log any communications that match exploits contained in its database or ruleset. Most can then be configured to email an administrator. Please note that an IDS is not a real time alert system. But, since most hacking attempts occur over several days, close attention to the logs should enable you to spot most attacks and take corrective action.

[6]Howard. p. 4

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Network sniffers work by recording all network communications and if combined with an IDS will help you to investigate any suspicious traffic or detected intrusion. However a good knowledge of TCP/IP is needed to make the most of these tools.

Conclusion

Securing Microsoft's Internet Information Server 5 can be a complex task. Hopefully I have given you a good start on securing your installation. This paper is by no means an all-inclusive document on security. Depending on your installation, additional steps may be required. I recommend that you read the references at the end of this paper. Security is not a "set it and forget it" task, you'll need to stay up to date. Therefore you should signup for the Microsoft Security Notification Service to stay abreast of all the latest security bulletins issued by Microsoft at the following URL

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/notify.asp

Another good resource for security news is Security Focus located at this URL

http://www.securityfocus.com/

Security Focus also hosts the famous BugTraq Archive. Security flaws for a wide range of products are normally posted to BugTraq.

List Of References

Cox, Philip. "Hardening Windows 2000". Windows 2000 Security Handbook. 1. 30 March 2001. URL: http://www.systemexperts.com/tutors/HardenW2K101.pdf (17 August 2001)

McClure, Stuart. Scambray, Joel. Kurtz, George. Hacking Exposed Network Security Secrets & Solutions. Berkeley. Osborne/McGraw Hill. 1999

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

Howell, Nelson. Forta, Ben. "Advance Security Concepts". (30 November 1997). URL: http://www.15seconds.com/issue/971130.htm

Burnett, Mark. "Ten Steps to a Cleaner Webroot". (12 June 2000). URL: http://www.securityfocus.com/focus/microsoft/iis/webroot.html

Sutton, Steve. Windows NT Security Guidelines. Urbana: Trusted Systems Services, 18 March 1998. 12

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: September 4th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
Security Leadership Summit & Training	Dallas, TXUS	Dec 03, 2015 - Dec 10, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced