Global Information Assurance Certification Paper

Securing a Windows 2000 IIS Web Server – Lessons Learned

Harpal Parmar October 8, 2001
SANS Security Essentials GSEC Practical Assignment (v.1.2f) (August 13, 2001)

Introduction

As more and more businesses go online, the demand for easy to implement, inexpensive web solutions substantially increases. The increased popularity of Microsoft solutions in the web server market can be attributed in part to this. There are many reasons why an organization would want to go with a Microsoft web server, as opposed to a Unix based Apache solution for example. Some of the more notable ones include:

Knowledge

- Most organizations have in house expertise with Microsoft products already. They may not have expertise in other Operating Systems and Web Servers.

Ease of Setup

- Some organizations may not have any dedicated IT personnel at all. Given the ease of the "point and click" setup, any individual familiar with Microsoft is likely to be able to set up a functional IIS web server.

Cost

- The cost of the hardware alone may force some organizations to go with a Microsoft solution. For example a decent Intel based box comes in significantly cheaper then a Sun box.

- Many organizations may already have the software and licenses already, so the cost of adding another server is not prohibitive.

Support

- Commercial products often provide better support for their products, whereas if you are running Apache, you are to a degree on your own.

One of the major advantages of going with a Microsoft solution boils down to ease of setup. As we've seen time and time again, ease of use is usually at the opposite end of the spectrum as security. Out of the box, an IIS server is not secure. Some may argue that Unix is more secure, but in my opinion a vanilla Unix install is not secure either, as there are many packages and services installed by default which you may never need or use. My Unix experience is by no means extensive, however I have found it less troublesome

to secure a Unix box then a Windows box. I actually come from a network background, dealing predominantly with routers and firewalls. Most of my Unix knowledge comes from reading books or watching over various (sometimes irritated) Sys Admins' shoulders and asking them questions. My current environment is Solaris, which combined with Linux is the basis of my limited Unix experience. My Microsoft server experience is limited as well, however the familiarity with Microsoft products is obviously fairly in depth from a user and networking standpoint.

After a merger of three companies, I am transitioning into more of a security role. One of the first incidents I had to deal with was the CodeRed worm. That feeling that I had in the pit of my stomache the first time someone came into the room and said "we've been hacked" is not something I will forget anytime soon. With my limited knowledge of Microsoft, I needed all the help I could get in securing an IIS server. I quickly realized that there are many different guides making many different recommendations. Unfortunately, some of these recommendations cause issues, therefore it is highly recommended that these recommendations be trialed in a test environment before being applied to your production environment. In an attempt to help you avoid some of the issues I encountered, the following details some of the quirks to watch for while securing your IIS server.

Building the Server

The installation of Windows 2000 is fairly simple. Services and components that didn't seem necessary weren't installed. We also shut down numerous services that we didn't think we needed. Installing Windows 2000 Service Pack 2 was easy as well, although I did run into one issue. The Service Pack installation insisted that the "Print Spooler" service must be running before it would proceed with the install. I'm still unsure why it needs the service running, but I was happy that it was nice enough to let me know I needed to turn it back on instead of giving a generic error and dying.

The next step was of course installing post SP2 patches for Windows 2000, as well as IIS patches. While this sounds simple enough, I quickly found it to be a daunting task. I found the list of patches to be fairly extensive. In some cases the "rollup" security patches do not include a listing of the patches that are included, so cross-referencing the patches became an annoyance. Microsoft makes a tool that came in very handy in identifying the patches that are recommended. The HFNETCHK utility will scan either the local system or remote systems for patches available for the following products:

Windows NT 4.0
Windows 2000
All system services, including Internet Information Server 4.0 and 5.0
SQL Server 7.0 and 2000 (including Microsoft Data Engine)
Internet Explorer 5.01 and later

This tool was beneficial in identifying a list of patches we should look into, and it worked

fairly well in most cases. I would recommend this tool not only for web servers, but also for your internal networks. It is available at:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/hfnetchk.asp

The Hardening Process:

There are many guides and tools available for hardening IIS servers. Some of the information found in one document will also be found in another. I usually try to amalgamate the points I think are relevant in our environment, so I gleaned relevant information from several documents into my own list. Below are some of the documents I used as a basis for what ultimately became my own checklist.

- The Secure Internet Information Services 5 Checklist available from Microsoft at:

  http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/iis5chk.asp

- "A Step-by-Step Guide to Securing Windows 2000 for Use as an Internet Server" by David S. Courington from the SANS reading room available at

  http://www.sans.org/infosecFAQ/win2000/win2000_sec.htm

- "SANS Security Essentials V: Windows Basics" from the Security Essentials Course

- The NSA Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0 available at:

  http://nsa2.www.conxion.com/win2k/guides/w2k-14.pdf

  The NSA also has some good security guides available. Although not in the scope of this document, I feel it is worth mentioning the NSA's "Router Security Configuration Guide". If you are looking for guidance in securing Cisco routers, this is an excellent read. It is over 200 pages, so if you don't have the patience to read it, take a look at the two page executive summary. Both are available at:

  http://nsa2.www.conxion.com/cisco/download.htm

Below are some of the issues we encountered (and you may encounter) while following some of the recommendations in these guides.

Services

Most of the guides recommend shutting down unnecessary services, including the "server" service. When we disabled the "Server" service, our "Virtual SMTP Server" configured in IIS disappeared. While the service disappeared, the functionality appeared to remain intact. We have had no problems with SMTP since disabling the "Server" service. If you chose to do this, you must configure your SMTP parameters before disabling the server service. You probably should have a dedicated SMTP server in your DMZ, not on the same box as your web server. In our case we were forced to temporarily combine the two for the time being due to some outside constraints.

Of course, the guides do not assume you are running SMTP on your IIS server. No guide is going to cover every configuration option you may be running. You have to try the recommendations and see if anything breaks.

Moving/Renaming Executables

"A Step-by-Step Guide to Securing Windows 2000 for Use as an Internet Server" guide recommends deleting, moving and/or renaming the following executables:

XCOPY.EXE	RSH.EXE
AT.EXE	FINGER.EXE
REGEDIT.EXE	RUNAS.EXE
CACLS.EXE	FTP.EXE
REGEDT32.EXE	RUNONCE.EXE
CMD.EXE	ISSYNC.EXE
REGINI.EXE	TELNET.EXE
CSCRIPT.EXE	NBTSTAT.EXE
REGSRV32.EXE	TFTP.EXE
DEBUG.EXE	NET.EXE
REXEC.EXE	TRACERT.EXE
EDLIN.EXE	NETSH.EXE
TSKILL.EXE	RCP.EXE
POLEDIT.EXE	WSCRIPT.EXE

I discovered some unexpected behavior when I attempted to move the executables. I would move the file, and verify it was gone from the \winnt\system32 directory. When I went to do a final verification, the files had magically reappeared.

After questioning my own sanity and swearing up and down that I was sure the files had been moved, I moved them again. The files reappeared again. After doing a search I found there was a hidden directory called \winnt\system32\dllcache, which contained a copy of the executables I was trying to move. Window automatically refreshed the deleted executables from this directory, and restored them to the \winnt\system32 directory.

I deleted some of the executables from the \winnt\system32\dllcache directory, and some of them would reappear in the \winnt\system32 directory again. I did a search for the executables and found another directory called \winnt\ServicePackFiles that contained copies of the executables, presumably updated files from patches that had been applied. After deleting the files in this directory, they finally stopped reappearing in \winnt \system32.

Once the files were moved to a different folder, we encountered another issue. One of the backend applications on the server had to be started via a batchfile, which depended on cmd.exe, which we had moved and renamed. We ended up renaming it back to cmd.exe, illustrating the balance we need to find between functionality and security. We are currently looking into alternatives to the batchfile scenario, so we can rename cmd.exe, enabling us to be slightly more secure.

Hisecweb Security Template

The Security Configuration Tool Set, which is installed as part of Windows 2000, consists of a set of Microsoft Management Console (MMC) snap-ins that allows administrators to configure security settings using customizable templates. One of the templates offered by Microsoft is the High Security Web (Hisecweb) template. This template is an inf file that you copy into the \winnt\security\templates directory. You can then open, modify and apply it using the MMC.

After applying the Hisecweb template available from Microsoft, I started experiencing a strange issue. Our webserver now took more than 10 minutes to reboot. After further investigation, I found Hisecweb template was clearing the pagefile from the hard drive at shutdown. Depending on the size of the pagefile, this can result in long reboots.

When using the Hisecweb template, it is a good idea to be familiar with the settings it is actually changing. Through the use of the MMC, you can view your current settings as well as the settings in the Hisecweb template. It is a good idea to use the template as a starting point, and then customize the settings according to your preferences. Alternatively, you can look at Hisecweb.inf via a text editor.

There is a decent guide available from Microsoft explaining how to use the Security Template, and how to create your own template. The “Step-by-Step Guide to Using the Security Configuration Tool Set” is available at

http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/deploy/confeat/seconfig.asp

Since my webserver is not running the Routing Remote Access Service (RRAS), I didn’t experience the following issue. I came across an article in the Microsoft Knowledge Base

which I thought would be important to mention.

If you are running RRAS and you apply the Hisecweb template, you will notice RRAS isn't running anymore. The following is from "Applying a Hisecweb.inf Template to a Web Server Prevents the Routing and Remote Access Service From Starting" (Microsoft Article ID: Q272978):

"If you apply a Hisecweb.inf security template to Microsoft Windows 2000 Server, the Routing and Remote Access Service is prevented from starting. When the service attempts to start, the following error is logged to the System Event log of the server:

> *Source: Service Control Manager*
> *Event ID: 7024*
> *Description: The Routing and Remote Access service terminated with service-specific error 711."*

"*This behavior is by design."*

The entire article is available at:

http://support.microsoft.com/support/kb/articles/Q272/9/78.ASP

Changing the IIS Banner

Microsoft web servers have been specifically targeted by recent worms (Sadmind, Code Red and Nimda to name a few). One way to help thwart attacks targeted at Microsoft IIS servers is to change the IIS banner. The banner is what identifies the web server you are running, and is one of the methods an attacker uses to identify vulnerabilities that may be present on your system. You can usually view the banner by telnetting to port 80 of your web server, or using an automated vulnerability scanner like Nessus. Nessus is a freeware scanner that I have found to be very useful. You will need a Unix box to run the Nessus server, although you can run the client GUI on a windows machine. Nessus is available at http://www.nessus.org.

I found the following discussion pertaining to changing the banner while doing a search on SecurityFocus.com:

http://www.securityfocus.com/cgi-bin/archive.pl?id=105&start=2001-10-03&end=2001-10-09&mid=146530&threads=1

This message is valuable in that it provides the pertinent file information necessary to modify the IIS banner. This can be achieved by using a hex editor to modify W3SVC.dll.

You can change the "Microsoft-IIS/5.0" string to something else, perhaps a bogus version

of Apache or some other web server, or you can make up your own. When we modified the dll, we would get an error message saying the dll was corrupt. What we ended up doing to get it to work was to ensure our bogus web server name was the same amount of characters as the original banner.

The author of the message referred to above (Hannes Jahn) goes on to state the following:

> *"But notice that there are many other ways to determine the victims OS, for instance using nmap's OS detection. So if a webserver runs a Redmond OS it's very likely also running IIS."*

This is a very valid point and should be taken into consideration. For fun, I tested to see if changing the banner would be sufficient to fool the CodeRed worm. I downloaded the Eeye's free Retina Code Red Scanner from

> http://www.eeye.com/html/Research/Tools/RetinaCodeRed.exe

We ran the scanner against the IIS test server with the modified banner. This test server was set up to be vulnerable to the ida buffer overflow vulnerability exploited by the CodeRed worm. We had purposly not put on the necessary patches to fix the issue. We ran the scanner which reported that our test server was not vulnerable to the CodeRed worm, so even though there are other ways of detecting the web server, the CodeRed worm seems to be looking for that specific banner. Actually, the more accurate statement would be that *Eeye's CodeRed Scanner* was looking for the banner. I would recommend checking out Eeye's web site. They have some good free and commercial tools available, as well as some very informative papers and detailed analysis on the CodeRed worm.

Conclusion

With Microsoft quickly becoming the dominant and more popular web server, it is also becoming the number one target for viruses, worms and hackers. Due to this, it is essential to be able to confidently secure the IIS web server. While there is an overabundance of information pertaining to IIS security, it often fails in identifying the many issues that can result. Some of the steps you take towards securing your web server may result in a loss of functionality. While it goes without saying that no guide is going to be able to cover every conceivable configuration, it is essential for those in charge of security to be familiar with their own environment. It is very important not to look at patches as a generic cure-all. What I've found to be effective is to adopt a trial and error approach when attempting to balance security with functionality, as you may experience many issues pertaining to your specific environment. Some of these issues have been outlined above and, hopefully, will aid you in avoiding some of the pitfalls that I experienced and ultimately save you some time.

References

Howard, Michael *"The Secure Internet Information Services 5 Checklist"* June 29, 2001
http://www.microsoft.com/technet/treeview/default.asp?
url=/technet/security/tools/iis5chk.asp

Courington , David S. *"A Step-by-Step Guide to Securing Windows 2000 for Use as an Internet*
Server" March 29, 2001
http://www.sans.org/infosecFAQ/win2000/win2000_sec.htm

Walker, William E. IV *"Guide to the Secure Configuration and Administration of Microsoft*
Internet Information Services 5.0" version 1.2 August 20 2001
http://nsa2.www.conxion.com/win2k/guides/w2k-14.pdf

Antoine, Bosmajian, Duesterhaus, Dransfield, Eppinger, Houser, Kim, Lee, Opitz, Wiacek,
Wilson and Ziring *"Router Security Configuration Guide: Principles and guidance for secure configuration of ip routers, with detailed instructions for Cisco Systems routers" version 1.0h* September 17, 2001
http://nsa2.www.conxion.com/cisco/download.htm

Cole, E; Wendt, Carla; Kolde J *"Internet Information Server (IIS) Security – SANS Security Essentials V:Windows Basics v1.2"* June 6, 2001

Microsoft Corporation, Microsoft's HFNETCHK Patch Status Utility
http://www.microsoft.com/technet/treeview/default.asp?
url=/technet/security/tools/hfnetchk.asp

Microsoft Corporation, *"Step-by-Step Guide to Using the Security Configuration Tool Set"*
http://www.microsoft.com/technet/treeview/default.asp?
url=/TechNet/prodtechnol/windows2000serv/deploy/confeat/seconfig.asp

Microsoft Corporation, *"Applying a Hisecweb.inf Template to a Web Server Prevents the Routing and Remote Access Service From Starting" (Microsoft Article ID: Q272978)* December 9, 2000

http://support.microsoft.com/support/kb/articles/Q272/9/78.ASP

Jahn, Hannes *"Remove IIS Banner (was server identification)"* November 23, 2000
http://www.securityfocus.com/cgi-bin/archive.pl?id=105&start=2001-10-03&end=2001-10-09&mid=146530&threads=1

Laurentiu, Nicula (Eeye Digital Security)*"The Retina CodeRed Scanner"* 2001
http://www.eeye.com/html/Research/Tools/RetinaCodeRed.exe

Nessus Security Scanner
http://www.nessus.org

Last Updated: August 21st, 2017

Upcoming Training

Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401**	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
Community SANS New Orleans SEC401	New Orleans, LA	Oct 23, 2017 - Oct 28, 2017	Community SANS
Community SANS Omaha SEC401	Omaha, NE	Oct 23, 2017 - Oct 28, 2017	Community SANS
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 30, 2017 - Dec 06, 2017	vLive
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Vancouver SEC401**	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS