Global Information Assurance Certification Paper

A More Secure Web Presence for Microsoft Networks
Michael C. Trammel
GSEC Practical assignment 1.3
March 26, 2002

Goal
The goal of this article is to provide administrators the facts needed to present an argument to management that Apache provides more security and less risk at a lower cost of ownership for the same training dollars. It will also attempt to make Microsoft administrators familiar with the general structure of Apache in order to assist them in their efforts to adopt this technology.

Introduction
Most large companies and institutions today have elected to standardize on one platform in an effort to lower total cost of ownership. The one platform idea has some proven advantages, such as economies of scale. This is the idea that instead of several small purchases of this and that, one larger purchase is made for the one platform that results in some volume discount usually in the form of a license agreement. Another advantage is the cost of training. Users, helpdesk personnel, and administrators all have to attend training for each platform and its specific applications. The dollar amount for this training can be better controlled if a limited number or single platform is utilized. These (and other) total cost of ownership factors lead many organizations to issue policies on standardization. One operating system and applications specific to that platform are specified and the employees are restricted to this range of options.

In and of itself, standardization is not a bad thing. The employees become comfortable with the technologies deployed and the network and computers fade into the background and become tools for productivity, instead of barriers to productivity and sources of frustration. In addition, dollars that would have been spent on training and platform specific software for second or third platforms is saved and can be used elsewhere. The CFO smiles.

A quick drive through Redmond Washington will make it clear which platform the majority of companies decided to standardize on. Microsoft operating systems and desktop software are used on over 90 percent of personal computers.[1]

Why Remain on a Microsoft Platform?
The Linux are Coming! The Linux are Coming!
Not exactly…with Microsoft's 90 percent established base, why not choose Microsoft. Odds are the people walking into HR with applications in their hand are already trained on Microsoft either because they run it at home or used it on previous jobs. Linux has received a lot of press regarding its closure on Windows, however, Larry Seltzer has a different view. He points out that, "the failure of companies like VA Linux and Dell to sell Linux desktops is a pretty clear sign that few people currently want to buy them."[2] Further more, Rawlson King points to a Goldman Sachs survey that indicates, "65 percent of executives in fortune 1000 companies had no intentions of using Linux for

their internal operations in 2002."[1] Companies that have invested large sums of money for company wide license agreements are not likely going to abandon working infrastructures and switch platforms. Doing so would involve costly retooling, retraining of employees on the new platform and its applications, and developing a completely new skill set in the IT department. So, odds are not good that people showing up at HR with applications will be Linux trained instead of Microsoft trained. Rawlson King points back to the Goldman Sachs survey to drive this point home, "Though Linux can be obtained for free, deployment of the operating system could potentially increase IT costs, due to the lack of solid groupware applications, and because of the increased technical support required to introduce a new operating system."[1]

But then there is the security issue. Linux is more secure than Microsoft is the battle cry of the Linux supporters and more than likely its true if you compare out of the box systems. However, by following published guidelines about how to harden your Microsoft system and by following a defense in depth mindset, the Microsoft platform can prove to be a formidable opponent to the would be hacker. Linux does not present enough of a security advantage over a properly hardened Microsoft system to warrant tossing out the investment in Microsoft licenses in favor of Linux. Not only does it mean abandoning the license agreement but you are also back to the issues of retraining staff, migration of data, and deploying new operating systems and developing new skill sets in the network administrators. Costs which are all pointless if you are already have an established Microsoft infrastructure.

Why Abandon IIS for Apache

Hook any IIS web server to the internet without any patches and its not 'if you get infected' its 'when you get infected'. Today there are still numerous machines still spitting Code Red, Code Red II, and Nimda either because the owner is oblivious to the infection or ignoring it for malicious reasons. It is a strong bet that sooner or later you will get probed and if not properly patched…infected. In an article published in Computerworld Online, Nicholas Petreley's web server logged "35,000 Nimda and Code Red probes" during a five day logging session![4] He goes on to state that not one probe was logged that related to Apache.[4]

Problem is that IIS has so many vulnerabilities that Code Red variants may be looking for holes you may not know about yet. Nimda is an example of this. It combines exploits such that if one failed… maybe others might work. It could spread by e-mail attachments, corrupt Internet Explorer downloads, and through IIS.[6] As of the day this document is being written, a search on vulnerabilities at Security Focus Online (www.online.securityfocus.com/cgi-bin/vulns.pl), found 86 known vulnerabilities for IIS compared to 26 for Apache over the same time frame (1996-present).[5] It is obvious which has the stronger code. The high number of IIS vulnerabilities combined with the severity of the exploits lead the Gartner Group to authorize this statement:

> "Gartner recommends that enterprises hit by both Code Red and Nimda immediately investigate alternatives to IIS, including moving Web applications to Web server software from other vendors, such as iPlanet and Apache. Although these Web servers have required some security patches, they have much better

> security records than IIS and are not under active attack by the vast number of virus and worm writers. Gartner remains concerned that viruses and worms will continue to attack IIS until Microsoft has released a completely rewritten, thoroughly and publicly tested, new release of IIS. Sufficient operational testing should follow to ensure that the initial wave of security vulnerabilities every software product experiences has been uncovered and fixed. This move should include any Microsoft .NET Web services, which requires the use of IIS. Gartner believes that this rewriting will not occur before year-end 2002 (0.8 probability)."[6]

Between Code Red, Code Red II, Nimda, and this Gartner Group recommendation, the internet saw administrators remove close to 150,000 IIS websites that were hosted on 80,000 Microsoft machines according to data in a Netcraft survey done in February of 2001.[7] Current numbers tell a better story. Current numbers indicate that in a physical count of web servers, 50 percent of those web servers are Microsoft platforms verses 30 percent that are Linux. However, in a logical count of websites, 65 percent are Apache and 26 percent are IIS.[3] These numbers made one author conclude regarding Microsoft, "…it takes 50% of the machines on the internet to run 28% of the websites."[4] It is my opinion that this author made an oversight. His statement assumes all Microsoft servers (making 50% of the web servers) run IIS (making 28% of the websites). Now, while I've yet to locate numbers to back this up, my wild best guess is that some of those Microsoft machines are actually adding to the Apache totals indicating administrators are heeding Gartner Group's advice. The same author I disagreed with a moment ago, however, best sums up this section when he stated, "Getting IIS free with Windows obviously doesn't mean it won't cost you in the long run."[4]

How to purchase and license Apache

The Apache license is one page in plain text format and it is in plain english. If you plan on using the software, take a minute to read this page at: http://httpd.apache.org/docs/LICENSE . It consists of 5 points, a legal disclaimer, a how to contribute section, and an acknowledgement. For those accustom to a Microsoft license, read this, it is refreshing.

This software is classified as freeware and costs nothing, however, the Apache Software Foundation states the following on its website:

> "As a volunteer-based organization, the Apache Software Foundation stands most in need of dedicated volunteers who can work on software, documentation, or administrative issues within each of the ASF projects, including the Foundation project itself. Other ways to contribute include providing services or equipment for use by the Foundation, or donating money to the Foundation."[8]

Information on how to donate time, software, or money can be found at http://www.apache.org/foundation/contributing.html#how-to-donate .

This is not a product you go to the store and purchase which may unnerve some Microsoft veterans. This is a download found at the Apache website and it includes PGP signatures and MD5 hashes to ensure clean downloads. Instructions for how to get started with Apache follow.

What risks are there to running Apache

There are risks to running Apache. To start with is the disclaimer published on the Apache Foundations site:

> **"Warning: Apache on NT has not yet been optimized for performance.** Apache still performs best, and is most reliable on Unix platforms. Over time NT performance has improved, and great progress is being made in the upcoming version 2.0 of Apache for the Windows platforms. Folks doing comparative reviews of webserver performance are still asked to compare against Apache on a Unix platform such as Solaris, FreeBSD, or Linux."[9]

This is a lovely disclaimer, however, based on sheer numbers of Apache implementations and the open source nature of the code, Apache is accepted as a proven piece of software.[12]

Apache is not a graphic program. It is controlled by a very powerful text configuration file which allows much more flexibility than IIS's GUI interface. Microsoft natives will find this to be a learning curve in the getting started process. The Apache Foundation is looking into a project to develop a GUI for Apache (release time frame is not certain) and there are also third party tools such as Plesk Server Administration, Samba, or Comanche.[10] Comanche appears to be the leader and can be downloaded at http://comanche.com.dtu.dk/ . Configuration of these GUI interfaces is not covered here.

IIS has the ability to administer multiple IIS web servers from a web browser, it can be setup using wizards and can be installed unattended…all of which are features the current Apache 1.3.24 lack.

Most of the argument for adopting Apache stems from lack of security in IIS. Apache has some known issues also, but on a much lesser scale. Not only are there fewer vulnerabilities, but they have far less sever repercussions. Apache for Windows is a relative newcomer to the stage so most likely there will be more vulnerabilities uncovered, however, unlike Microsoft, Apache has open code hence its unlikely that it will suffer any major hits. Most all of the known issues can be seen at Security Focus Online at http://online.securityfocus.com/cgi-bin/vulns.pl . The Apache Foundation website at http://www.apache.org/dist/httpd/ has a site for two types of patches. One is called contributory patches and is a directory of patches sent in by users and are issued on an as is bases…the other type are official patches developed by the Apache Foundation itself. The model Apache uses is to list patches until the next release of Apache comes out. The new release fixes all known bugs so there is no need to apply a stream of back patches or service packs! The official patches can be found at http://www.apache.org/dist/httpd/patches/ .

Before Starting to Install Apache

This next paragraph is the obligatory terms and important notes section. It is important to be familiar with the following before proceeding.

- Windows environments use .zip files for compression while most *nix machines use .tar. Unless complicating simple issues is enjoyed, Microsoft users should stick to the .zip files.
- Since Apache is open source, two download types exist…those with the source code included (indicated as src) and those without (indicated as no_src). The source code is in the C language and is not needed to execute Apache. If you know C and are curious or wish to compile the code you'll want the source version. For the highest compatibility, use Visual C++ 5.0 as this is the defacto standard for compiling on Windows. If you do not know C or do not intend to compile code, then the no_src version is a faster download.[13]
- In addition to choosing src or no_src, you must also choose between .exe or .msi. The .exe files relies on a setup program while the .msi relies on the Windows Installer. The .msi files are faster downloads but there is a catch. Your Windows version must support Windows Installer version 1.10 or better. It is shipped with ME, 2000, and XP. Users from 95, 98, and NT need to go to the Microsoft site to download the Windows Installer version 1.10 or better. Full instructions and website locations can be found under the MSI Binary Distribution Packages section at the website http://www.apache.org/dist/httpd/binaries/win32/ [13]
- Apache requires Winsock2 for TCP/IP to function correctly. Windows 95 users will need to upgrade their Windows Sockets version by going to http://www.microsoft.com/windows/downloads/bin/w95ws2setup.exe before proceeding with the install. All later versions of Windows shipped with version 2.0.[13]
- Apache's software has three numbers such as 1.3.24. The first release of Apache was 1.1, then 1.2, and the current 1.3. There is a next generation of Apache in the eaves known as 2.0, but is not tested well enough as of this writing to be considered production. The last number tracks bug and vulnerability fixes. Current versions of Apache are
  - 1.3.24 production
  - 2.0.32 beta
- XP users may encounter a known bug present in 1.3.23, but believed fixed in 1.3.24. If XP users encounter garbled output then they may be victims of this bug. The issue stems from Apache/Windows interaction and is being addressed by Microsoft. A Microsoft knowledge base article number Q317949 has been assigned to this issue, but is presently unpublished. For more information regarding this see the section Windows XP Apache Users Read this First at http://www.apache.org/dist/httpd/binaries/win32/ or search for the article referenced above.[13]

Requirements

There are some prerequisites to running Apache[9]

- Winsocks2 as mentioned above.

- If using the .MSI installation method, then Windows Installer 1.10 or better is required. The .EXE files sets things up and then installs using the Windows Installer so either method requires WI 1.10 or later.
- TCP/IP is mandatory
- Apache is designed to run on NT and 2000, while it will run on 9x it is not tested by the Apache Foundation, but is considered stable by its millions of users.
- For NT users please note. Apache requires Service Pack 3 or later officially. Unofficially Service Pack 4 created some issues with TCP/IP and WinSock integrity that were corrected in SP 5. It is suggested that SP 5 or later be used.[9]
- Apache can not share ports with any other process. Its is suggested that you use the netstat tool to determine if anything is operating on port 80 prior to installation. If there is a conflict, either the existing program must be moved or Apache configured to use a different port.[9]
- This final prerequisite is not in any of the documentation but is important anyway. If you are on a company network, check with and obtain permission from the network administrator that you are authorized to post a website. Some company policies forbid this activity and may carry consequences.

Installation

The best source for Windows Apache downloads is at Apache itself. The download site for win32 is at http://www.apache.org/dist/httpd/binaries/win32/ , there are other options including older versions and the 2.0 beta version located at http://www.apache.org/dist/httpd . The download site also has the PGP signatures of the download files. The PGP signature can be used to check that the downloaded file is not corrupt and that it does not contain hidden hackerware. For full instructions on how to utilize the PGP signatures, see the instructions at the bottom of the page http://www.apache.org/dist/httpd . If you are not familiar with PGP or MD5 (another verification method) understand that these steps are optional and Apache's function will not be affected by them assuming a clean install occurred.

For the purposes of this how to section, Apache 1.3.24 is selected and downloaded. Specifically, "apache_1.3.24-win32-x86-no_src.exe" and "apache_1.3.24-win32-x86-src.msi" will be looked at.

Either version can be launched simply by double-clicking the icon. When launched, the .EXE version shows the progress bar as the setup program initializes the Windows Installer and then (on an out of the box Windows 2000 Advanced Server) reports that Windows Installer 1.10.1029.0 was found and that it is not the up to date version, but since it meets prerequisites the install continues. From this point on, the Windows Installer is in control and both the .EXE install and .MSI install worked the same.

At this point you should see this screen.

By clicking Next, the License agreement screen will come up asking if the license agreement is acceptable. Note that not accepting the license is the default and that I accept must be selected before the Next button becomes available.

- Select *I accept the terms of the license agreement*
- Click **NEXT**

This brings up a Read this First box. Look over the notes before proceeding

- Click **NEXT**

Next is a Server Information box. It asks some important questions that help configure Apache. Seek your network administrator's assistance if you are not familiar with the names it requests. The second section on this page asks how you plan to run Apache. Note: If you run Apache as a service then it is started automatically and is available for every user. If you start it as a console (by choosing "Run when started manually, only for me (name)", then Apache is only available when you log in and issue a command to start the service. You must remain logged in and the console must remain open while Apache runs.

- Enter the appropriate names
- Select *Run as a service for All Users – Recommended*
- Click **NEXT**

Setup Type is the next box. It is recommended that a complete install be used as it will install all the documents and help files, source code, and the actual application. All that is needed is the Apache runtime portion, but for inexperienced administrators, the help files are invaluable.

- Select *Complete*
- Click **NEXT**

Destination Folder dialog box follows allowing a change in the path to where the software will be installed. The default path is c:\program files\apache group\apache.

- Accept the default

- Click **NEXT**

Here is the last chance to change the settings from the wizard. When happy with the selections made

- Click **Next**

The files are copied and the wizard indicates completed.

- Click **FINISH**

Congratulations, the server is now an Apache Web Server. Next step will be to test the configuration for errors and this can be done either of two ways.
First go to Start | Programs | Apache HTTP Server | Configure Apache Server and select *Test Configuration*. This will generate error messages if the configuration file has any errors and these can be reviewed under Start | Programs | Apache HTTP Server | Review Server Log Files by selecting *Review Error Log*. The second part of the test is to go into the web browser and go to website http://localhost/ or http://127.0.0.1/ . You should receive this screen if all is working properly.

If this does not appear, repeat the first test above and examine the error log. It should give a good indication of what is wrong. If it did appear, not only do you have an Apache Web Server, but it is ready for your content.

There are three directories that need to become familiar at this point if you installed the complete version. The three directories are as follows:[14]

- Source Directory – Location of the source code for the Apache Software
  - C:\Program Files\Apache Group\Apache\Src
- Server Root – Location of the Apache executable
  - C:\Program Files\Apache Group\Apache
- Document Directory – Location of the documents that will be served to the web
  - C:\Program Files\Apache Group\Apache\htdocs

The document directory is where all the excitement takes place. Its named htdocs and in it is a list of files called *index.html.??* The question marks represent wildcards that can be replaced with other letters. Index.html is the default website. The last two letters are

the language that the website is in. If you need French, choose index.html.fr and for English, choose Index.html.en. The last screen grab shows the contents of Index.html and FrontPage will edit it easily.

One thing to keep in mind with htdocs is that it is the default location specified by Apache installs. It is not a bad idea to move the folder or use a different one all together. To accomplish this, you'll need to visit httpd.conf file. It is located at C:\Program Files\Apache Group\Apache\conf\httpd.conf. If you have ever used IIS and gone to the Microsoft Management Console and right clicked on the server name and accessed the properties for the server as a whole and then done the same for any web site on that server…this file is the equivalent on steroids! Much more control and flexibility is built into this file than IIS GUI can pack. If you move the htdocs folder or rename it, you will need to replace all references to it in httpd.conf with the path to the new location or folder.[14] If you change the name of the index.html file, this is where you will need to change that reference as well. Find and replace works wonders here.

The Apache web server is now installed and the basics should be understood. One good part about Apache is its modular structure. If you need to add services to it, they are not all inclusive so you can add only those you need and not expose the server to unneeded open ports on unused services. If it comes bundled with services you do not need, they can be removed. For a list of all modules included with the Apache distribution see http://httpd.apache.org/docs/mod/index-bytype.html . Additional 'non-official' modules are available on the web, though it is never suggested that they be used in production unless thoroughly tested and inspected, however, there are legitimate modules out there. If you need extra services, the best site to look to for more information is at http://tud.at/programm/apache-ssl-win32-howto.php3 . This page tells how to install SSL support on the Windows Apache platform and gives clear instructions that will get you familiar with the process. Most other modules will be loaded in a similar fashion.

The cost of training a person on Apache is low. Being familiar with IIS, this author learned it over a weekend and once I was familiar with the file placement in Apache, I had no trouble implementing the server. All of the information needed is on the Web, however, some text books do help. There are two I have come to rely on "Installing and Configuring Web Servers Using Apache" by Melanie Hoag by Wiley publishers ISBN#0-471-07155-2 and "Apache Server for Windows Little Black Book" by Matt Keller, Matthew Keller, and Greg Holden by the Coriolis Group ISBN# 1576103919. Both these books are invaluable if you plan to support production machines.

Conclusion:

IIS presents a security risk to any organization using it. It has a high number of known vulnerabilities that have severe exploits such as Code Red and Nimda. Companies today like to standardize in hopes of saving money and often mandate policy without fully understanding the ramifications. IIS may not be the best tool for the job when it comes to websites. While it comes bundled with Windows and is in essence free, the cost of maintaining the server and shielding it from the constant probing and the cost of training technicians to perform these tasks is not free. Apache is not risk free, but does present a

smaller target in that there are less than half as many known vulnerabilities and these are far less dramatic than those on IIS. Purchase cost for Apache is the same as IIS, free. Training the technician to use the product is comparable to IIS, but securing the machine is far less costly in technician time and the amount of shielding needed…Apache is not under the constant probing and infection risks IIS gets. Bottom line, Apache is a more secure web solution for Microsoft platforms than IIS.

References

[1] Rawlson King, Linux Market Share Within Web Server Sector to Grow, January 7, 2002 URL: http://thewhir.com/features/linux-market-share.cfm

[2] Larry Seltzer, Linux Threatens Unix, Not Windows, October 3, 2001 URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2816323,00.htm

[3] Netcraft, Netcraft Web Server Survey, February 2002 URL: http://www.netcraft.com/survey/

[4] Nicholas Petreley, The Cost of Free IIS, October 22, 2001 URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO64914,00.html

[5] SecurityFocus Online, Vulnerabilities, as of March 24, 2002 URL: http://online.securityfocus.com/cgi-bin/vulns.pl

[6] John Pescatore, Nimda Worm Shows You Can't Always Patch Fast Enough, September 19, 2001 URL: http://www4.gartner.com/resources/101000/101034/101034.html

[7] James Middleton, 80,000 Microsoft Servers 'disappear', February 10, 2001 URL: http://www.vnunet.com/News/1125766

[8] The Apache Software Foundation, Contributing to the Apache Software Foundation, as of March 25, 2002 URL: http://www.apache.org/foundation/contributing.html

[9] The Apache Software Foundation, Using Apache with Microsoft Windows, as of March 25, 2002 URL: http://httpd.apache.org/docs/windows.html

[10] Raj Rajagopal, Comparing Apache and Internet Information Server, December 4, 2000 URL: http://www.networkcomputing.com/unixworld/1124/1124uw.html

[11] Rich Bowen, Apache on Windows, October 23, 2000 URL: http://apache.rcbowen.com/ApacheOnNT.html

[12] The Apache Software Foundation, Apache Server Frequently Asked Questions, as of March 25, 2002 URL: http://httpd.apache.org/docs/misc/FAQ.html#tested

[13] The Apache Software Foundation, Important Notices, as of March 26, 2002 URL: http://www.apache.org/dist/httpd/binaries/win32/

[14] Ken Coar, Getting Started with Apache 1.3, June 1, 2000 URL: http://www.bretoned.ca/iei/tutor1.htm