Global Information Assurance Certification Paper

SANS Security Essentials
GSEC Practical Assignment
Version 1.2f (amended August 13, 2001)

Researching a Topic on the Internet:
Apache on Windows as an alternative to Internet Information Server

Eve Edelson
October 19, 2001

Abstract

Many systems administrators use Internet Information Server to host web sites because it is free and bundled with NT servers, comes with many configuration and publishing tools, and because its presence is necessary to certain other Microsoft products such as Exchange Server. Because of growing concern about its security, however, and the workload associated with its support, administrators with a stable of Intel boxes may be considering alternative server software. A web server should be affordable, stable, secure, relatively easy to install and maintain, and compatible with typical applications such as cgi programs, database interaction and virtual hosting. Support and a sizeable user community are desirable. Based on these criteria, Apache is a credible alternative to IIS as a Windows-based server. The comparison is made for an office environment with a small budget and support staff. This paper does not compare operating systems (although Apache is more commonly seen on Unix boxes) or address open source issues, and it is assumed that buying new hardware is not an option. Information was drawn from internet sources, colleagues and the author's experience.

Basics of Apache and IIS

Netcraft [1] reports that Apache accounts for about 60% of large servers (hosting more than 5000 sites). IIS accounts for 27%. Slightly less than half of the servers running Apache host .com domains, while two-thirds of servers running IIS host .com domains. This reflects the dominance of IIS in the business world. More than half the web servers defaced since late 1999 were running Windows NT - which probably means they were running IIS, as Apache is more commonly used on Unix platforms. 24% were running Linux (which probably means they were running Apache) [2].

Apache is a free web server package from the Apache Software Foundation [3] which runs on most operating systems (and is bundled with many). Configuration usually involves editing one file. Free graphical tools are available as add-ons. While the default installation is sparse, modules for, e.g., php or SSL can be added.. Apache is widely used with mySQL (a free database product) for web-enabled database access. It supports scripting with such languages as JavaScript, and CGIs in any programming language. The Apache Software Foundation does not officially support Apache: no one is 'liable' for faults in the software. Despite this, Apache has a large user community.

IIS (Internet Information Server) is a Windows-only web and ftp server package which comes with Windows NT. It has a fully-integrated graphical administration tool for creating virtual web and ftp sites. It supports CGIs in any language supported by the host OS (e.g., perl, Java, C), and 'universal' scripting languages such as php and JavaScript. In addition, IIS supports ASP, Microsoft's scripting technology, and scripting in VBScript, Microsoft's proprietary scripting language. Microsoft has provided development tools for buildingWindows-based web sites and integrating IIS with their other products (SQL Server, etc.), indeed IIS is integral to certain other Microsoft packages such as Exchange.

Both packages can support institutional (e.g., heavy) traffic.

Security

Apache

Apache's default installation is sparse, on Windows and Unix (Linux distributions may be different and are not dealt with here). By default, few server extensions are installed. Apache runs with minimum privileges, which to some extent limits the damage from bugs

such as buffer exploits. It is still important to configure Apache to minimize the chance of site attacks involving, e.g., malicious form input, invocation of system commands, etc. CGIs must be written so that a malformed URL does not cause unexpected/undesirable results or reveal filesystem contents.
Configuring virtual hosts is easy in principle, involving adding a handful of lines in the httpd.conf file. In fact it takes a bit of thought, especially if separate access and error logs are desired for the virtual hosts, and sometimes it does not work right off the bat. Newsgroups such as comp.infosystems.www.servers.ms-windows are full of cries for help from people who can't make their virtual hosts work as expected. Some of these folks haven't read the directions but others are confronting real mysteries.
Apache does have security-related bugs, but fewer than IIS, and patches are available. The latest Apache issue of concern on Windows is a bug in version 1.13.20 which could allow an overlong URL to cause a buffer overflow. This is supposed to be addressed in 1.13.21 (not ready at time of writing). There have also been a few denial-of-service problems and bugs allowing files or directories to be listed when they are not meant to be.
To the vulnerabilities of Apache must be added those of the operating system. Systems must be kept updated, and configured so that, for instance, scripting language interpreters (e.g., perl) and user directories are located safely.

To the extent that open source development promotes the hardening of Apache, open source may indeed be a good thing. However, DNS and FTP source code are open and have holes. Therefore open source is not considered in and of itself to be good or bad for the purposes of this comparison.

Internet Information Server

Running IIS means running Windows. The product is powerful but the NT and IIS permissions schemes are integrated and complex. In meeting the noble challenge of providing a graphical administration interface, Microsoft has provided an almost too-rich graphical environment for configuring virtual web and ftp sites. The most secure configuration is basically a web server with no other services running, no remote access and no virtual hosts. This is a showstopper for an organization serving a number of internal groups, all wanting separate web sites. In addition, the author has found that permissions (in NT) sometimes seem to break of their own accord. Patches come out often, sometimes break other patches and are not always detected by patch-checkers.

IIS runs with system privileges and the author is not aware of any way to alter that. Its default configuration needs significant changes right away, which should be done offline to avoid attacks [4]: installation on a non-root partition (not the default choice); the removal of default sample pages; careful permissions setting; renaming the IUSR and IWAM accounts and removing them from the Guests group, deleting the printer's virtual directory, deletion of \IISADMIN, minimization or removal of Front Page extension permissions, removal of certain application mappings such as .ida, de-activation of unnecessary services, etc. There is also an option for IIS address filtering, although this seems execessive for a web server intended to serve the public. It can also be used to block ip addresses of other internal IIS servers which may have been compromsed. The fact that this was recommended in a security workshop attended by the author says something about the anxiety level of IIS administrators [5].

A typical packet-based firewall will not catch typical web server attacks which send malicious "arguments" along with a URL, because it only checks source and destination ip addresses and ports, not the data in a packet. Many attacks to IIS allow an intruder to find out web server configuration information, and access files outside the web directory. A number of exploits are directed at ASP, Microsoft's scripting technology which is used for dynamic and database-enabled web sites. ASP source code may include database names and passwords. Another hack, known as the HTR exploit, involves retrieving the "global.asa" file which also contains information about database names and passwords. DLLs which are vulnerable to buffer overflows can be sent strings which are then executed with system privileges. [6]

If IIS is run on a box which is also a domain controller, web users are authenticated as domain users. This may be a security hole. Also, IIS does not always reliably restrict filesystem access to sanctioned directories. IIS has built-in SNMP support, another rich

feature, but one which makes it vulnerable to SNMP attacks. In IIS 4.0, default.asp pages can be exploited to alter source code. A host of malicious methods are available for exploiting vulnerabilities to malformed URLs. FrontPage extensions can be subject to a denial-of-service attack using a malformed URL, which can bring the server down. There is a patch for this, but it and the issues above are mentioned to show that keeping up with the hackers is time-consuming.

Finally, unauthorized users can access cached files without authentication if more than one virtual server is being run on a box. The solution is to run only one IIS server on a box, which seems to defeat the purpose of having a powerful CPU, operating system and web server.

All of this omits the barrage of viruses, trojans and worms launched at IIS such as Code Red, SIRCAM and Nimda. The author has had the pleasure(?) of seeing typical attacks of this sort aimed at a Windows box running Apache [7].

Microsoft has developed a universe of software and a comprehensive development environment to support businesses, and has the lion's share of the business software market. It is striking that a corporate IT oriented website such as ZDNet would now describe IIS as having the "the reputation of having more holes than Swiss cheese" and write that "Apache HTTP Server has earned what many hope for and few achieve: an enviable security reputation." [8].

Convenience (installation and configuration)

This is closely tied to security concerns, because IIS should be secured right out of the box.

IIS is a large package with many features. Its default installation includes a number of DLL extensions, all of which require occasional patching, and the many and varied steps needed to secure IIS were covered in the section above. Sometimes even if extensions are removed, some may be restored automatically when other components (e.g., FrontPage) are removed.

IIS can be up and running fast - if security is neglected. Virtual hosts are in principle easy to set up, but in fact the user interface is a bit confusing. If third-party software is installed to work with IIS, for instance a collaborative package such as DocuShare from IBM, its configuration may involve a lot of work, since third-party install manuals usually assume a default configuration which may either be undesirable from a security standpoint or inconvenient on a certain box. In such a case, non-trivial (and non-obvious) adjustments may be required in IIS, which technical support staff of the third-party vendor may not be equipped to support.

Hotfixes are not always simple to find, but are simple to install. However, this author has found that HFNetChk, the free utility which checks for hotfixes, does not always recognize when a hotfix has been installed. Sometimes a new hotfix will cause it to think an old hotfix is no longer present. This may be because the old hot fix is obviated by the new one, but the output of HFNetChk is barebones and not always clear. As with so many other Windows installation experiences, it is not always simple to tell what has been installed where, and which "leftovers" can be safely removed.

Apache configuration is easier to grasp, because it involves editing a single file, httpd.conf. (Formerly three files were involved, but these have been subsumed into one. Even then, it was pretty easy to grasp what was going on.) Certain security steps can be made fairly easily: installation on a non-root directory, relocation of user files, restriction of CGIs to a suitable directory, etc. Virtual hosting, both name and ip based, is fairly simple to set up, requiring some extra lines in the httpd.conf file (but see the caveat above in the security section).

Compatibility with other applications

Users often wish to develop web-enabled databases. This can be done using free-standing programs in perl, php, C, etc., which is supported by both Apache and IIS, or Microsoft-specific technologies and products, e.g., ASP scripting and Access or SQL Server databases. It is not necessary to run IIS to use ASP scripting on Windows against databases, be they Microsoft products (Access, SQLServer) or other (mySQL). This author has done scripting in VBScript and php against Access and mySQL on Windows running Apache.

Another consideration which may limit choice is that IIS is integrated with Windows and is necessary for running a number of other services such as Exchange.

However, code which does run against Apache servers, e.g., perl or php, can be ported to other platforms without much if any modification, whereas ASP code must be rethought entirely if moved off a Windows platform.

Cost

Both Apache and IIS are free. The differential cost, then, is the cost of labor, for installation and ongoing maintenance, support of users, plus the cost of any downtime. The author's experience is that Apache is less work to set up, and to maintain. Both products are pretty stable. The author has found that the permissions on various virtual sites (web,ftp) within IIS sometimes break for no obvious reason. This experience has been erratic, but time-consuming when it does occur. Another consideration is the ease of upgrading. Upgrading Apache is fairly straightforward; upgrading IIS can have unwanted effects on permissions. IIS is so integrated with the rest of the Windows operating system that changes in IIS can have unexpected effects which are time-consuming to track down. IIS comes with features which are supposed to help users publish their sites (e.g., FrontPage), and the ASP scripting feature can be a powerful tool to help people develop their own interactive sites. However, the administrator will also have to support any such features regardless of platform. Overall, the labor cost of Apache seems lower.

Future prospects: patches, user community

In choosing a web server, the administrator needs to feel that the product has a future, in the form future software updates to deal with any needed enhancements to keep up with technology, and patches to deal with any shortcomings in those enhancements. Patches are reliably available for both Apache and IIS (in the case of IIS, they are frequent).

There are lots of newsgroups and other forums devoted to Apache and IIS where problems & solutions can be shared, and a robust industry devoted to supporting both user communities with technical support and third-party software for administering and extending servers. The Windows/IIS community is bigger, and support is available at all levels of experience. There is no shortage of books about either product.

Conclusions

Based on security, ease of installation and configuration, cost (including the cost of labor and any external software or hardware needed to beef up security), and future prospects (including availability of software updates and existence of a sizeable user community) Apache is a credible alternative to IIS on Windows. It is not without drawbacks, but a systems administrator looking for new directions should give it consideration.

References

1. Netcraft Survey Results, http://serverwatch.internet.com/netcraft/200109netcraft.html September 2001 Netcraft Survey Highlights of Web Server software usage on the Internet based on responses from over 32 million sites.

2. Attrition.org: http://www.attrition.org/mirror/attrition/os-graphs.html Defacements by operating system, 8/99-2/01.

3. Apache Organization: http://www.apache.org

4. http://www.lbl.gov/ITSD/Security/guidelines/websecure.html Lawrence Berkeley National Laboratory Computer Protection Program Web and FTP Server Security

5. "Securing IIS Web Servers", a course taught by Eugene Schultz at Lawrence Berkeley National Laboratory, September 2001, supplemented by SANS Institute http://www.sans.org

**6. http://www.clicknet.com/products/entercept/whitepapers/wpfuture.asp
Entercept Security Technologies, The Future of Web Server Security (Yona Hollander) (2001)**

7. Diary of a Mad Web Server (ip numbers changed to protect the pathetic):

```
-------------------------------------------------------------------------------------------------------------
xxx.xxx.xxx.xxx. - - [19/Sep/2001:15:04:25 -0700] "GET
/scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 301
xxx.xxx.xxx.xxx. - - [19/Sep/2001:15:04:25 -0700] "GET
/scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 301
xxx.xxx.xxx.xxx. - - [19/Sep/2001:15:28:56 -0700] "GET /scripts/root.exe?/c+dir HTTP/1.0"
404 279
xxx.xxx.xxx.xxx. - - [19/Sep/2001:15:28:57 -0700] "GET /MSADC/root.exe?/c+dir HTTP/1.0"
404 277
xxx.xxx.xxx.xxx. - - [19/Sep/2001:15:28:57 -0700] "GET /c/winnt/system32/cmd.exe?/c+dir
HTTP/1.0" 404 287
xxx.xxx.xxx.xxx. - - [19/Sep/2001:15:28:58 -0700] "GET /d/winnt/system32/cmd.exe?/c+dir
HTTP/1.0" 404 287
xxx.xxx.xxx.xxx. - - [19/Sep/2001:15:28:59 -0700] "GET
/scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 301
-------------------------------------------------------------------------------------------------------------
```

8. (http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2792860,00.html, July 2001)

Last Updated: July 24th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
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 Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
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 Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
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
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor