Global Information Assurance Certification Paper

Jonathan Davies
GSEC Assignment v1.4
October 2002

Security Considerations for Sharepoint Team Services on Windows 2000 server

1. Abstract

Microsoft Sharepoint Team Services (STS) is one of a number of “web based” products being offered as collaborative tools for the sharing of information. This information sharing could be both internally and externally, the latter being either to allow access to remote users or for collaboration with clients and/or business partners. If cost and simplicity are the main concerns then the most likely implementation of STS in a server based environment will be a single server running Windows 2000 server with IIS5 (and for this paper it is assumed that the database backend will SQL Server 2000). STS can also be run on other versions of Windows, namely NT4.0 server and workstation and Windows 2000 professional, and most of the information contained within the document will also be relevant for these Operating Systems (with some minor adjustments). In addition, STS can be run on a Linux based Apache web server, which will require some different actions or procedures to those listed below although the principles described within the paper should be applicable.

This further enhancement to the Microsoft Frontpage Server Extensions, as with any web server based application requires some generic security considerations and some specific to the application. This paper includes both and is intended to provide pointers to anyone looking to implement an STS solution. These considerations can be applied equally to internal or external facing services, as the threat of attack does not always come from an outside source!

2. Technical Overviews

2.1 A Brief Introduction to Web server Attacks

Since the "World Wide Web" became easily accessible and its popularity as a source of information and entertainment took off, the servers providing this infrastructure (especially web servers) have also become the popular target of hackers. This is evident from data shown on the Incidents.Org website where the “Top 10” of attacked ports is displayed (http://isc.incidents.org/top10.html). This shows graphically the level of attack on the 10 most attacked ports over the

previous 30 days and port 80 (http) traffic is invariably one of the ports most consistently attacked (and usually it is at the top) [1].

The choice of attack on a web server is varied and offers the hacker two main goals; defacement or Denial of Service (DoS). Defacement simply means replacing or amending the contents that should be displayed on a website in order to display whatever the hacker chooses, whereas Denial of Service aims to block all access to the website for visitors and/or customers. When this occurs on a site conducting "ebusiness" the losses due to the site being unavailable can be measured per minute (and can be extremely large indeed). A further development of the DoS attack is the Distributed Denial of Service (DDoS) attack. This works by using a number of vulnerable machines, which are "infected" with a DDoS program, and then launching the attack simultaneously from many or all of these on the chosen victim. DDoS has an advantage for an attacker over a standard DoS attack, as was seen when the web servers of Yahoo were attacked in February 2000. The reason being that, rather than easily being able to identify and block the attacker by their IP address, the attack was being simultaneously undertaken from a number of machines [2].

2.2 Sharepoint Team Services - What is it?

STS is solution built on the latest version of "Frontpage Server Extensions" (FPSE) allowing people to "contribute to the team Web site using nothing more than a Web browser" [3]. Contributions can be in a variety of forms including documents, items for discussion, announcements, tasks and notable dates or events.

For a server to run STS it requires a number of separate entities:

- The Server Operating System (Windows 2000)
- The Web server Software (IIS5)
- The Database backend (SQL Server 2000)
- The "Application" (STS/Frontpage Server Extensions 2002)

Each of these items will have their own set of security considerations and "best practices".

A very handy resource listing all the Knowledge base articles for Sharepoint Team Services can be found on the KBAlertz website at http://www.kbalertz.com/technology.aspx?tec=184 (there is also a specific section for Frontpage Server Extensions 2002 entries at http://www.kbalertz.com/technology.aspx?tec=62). Included in these articles is information on security matters such as Service Packs. STS is a part of Office XP and consequently is updated using Service Packs for this product. (At the time of writing Office XP Service Pack 2 is the most recent).

3. Securing an STS Implementation

There are various methods and options available for securing your STS environment. The first two to be discussed will be patching and hardening, while the third section will provide some further options for securing the infrastructure. The extent to which these options are adopted will depend upon your requirements and budget! Although a Firewall is mentioned in the "Additional Options" section (as you may not feel you require one if you are only planning to rollout STS internally) it should be considered to be a minimum requirement, together with patching and hardening, for the security plan of any Internet facing network device.

One concern with STS is that the database username and password used by STS to connect to the backend database are stored unencrypted in the registry (rather ironically under the “Secure” key). Each Team Site also has its own key below the HKLM\Software\Microsoft\Shared Tools\Web Server Extensions\Secure key in which the username and password for the particular team site connection are stored (this is if you wished to use different usernames and passwords for the various databases and their related STS connections). This key is named in relation to the reference number of the virtual server the STS site is running on (eg LM/W3SVC/1:). If the information in these keys could be read easily, it gives the attacker a valid username and password for the SQL server without really trying.

Don’t forget Backup and Anti-Virus software! This is as much a part of your security strategy as the patching and hardening.

3.1 Patching

“Patches are programs that fix errors in software“ [4] the article ‘Operating System Security: Adding to the Arsenal of Security Techniques’ by Dave Ferraiolo and Peter Mell explains. Patching is the technique of applying or installing these fixes to software (Operating Systems, applications etc).

Frequently, but not always, these patches are released to fix Security holes and they can come under a host of names and guises, e.g. patch, hotfix, service pack. Having all these different terms could be confusing and hopefully things should soon be getting easier as “Microsoft is developing a long-term plan to unify the process of installing various software updates across its product groups” [5].

Two products have made available by Microsoft that can be used to check whether all available patches have been applied to a server – hfnetchk and the Microsoft Baseline Security Analyzer (see Available Tools section below).

3.2 Hardening

Hardening is the process of securing a server. Hardening a server could involve turning off unused services and applications, and/or restricting access to applications or files (including the registry). Like many of the other options listed, can be applied to varying degrees and how much of the hardening you apply will depend upon your requirements. It is good to start with a "best practices" document and then see if any other additional hardening is required.

Frequently during hardening you may find that your service (or application) stops working. It is always good practice to apply a small amount of settings at a time on your first attempt to harden a server and test each time settings have been applied (this makes it much easier to work out which setting broke the service should that happen). You should document each of the settings for the next time you (or someone you hand over to) will have to do it, also noting which settings should not be applied because they broke the service. If possible, once you have ascertained all the hardening you wish to take place, script the application of all the settings you require.

3.2.1 Windows 2000 Server

The first thing to ensure when installing your Windows 2000 server is that it uses the NTFS file system (a FAT file system does not have the capability to be run securely). The Windows 2000 install will probably find a lot of services running that you have no requirement for – disable them. Also disable accounts that you are not using (such as guest) and it is good practice to rename the administrator account to a name that does not advertise its capability, and then create a new account called administrator that has no permissions (and give it a ridiculously difficult password to guess). All passwords should be "strong", ideally containing numeric characters (and not just at the beginning or end).

Microsoft have produced a Windows 2000 Server Baseline Security Checklist, which is a good place to start looking at for further options and it can be found at http://www.microsoft.com/technet/security/tools/chklist/w2ksvrcl.asp. Included in it are links to other documents with further information. The Hacking Exposed: Windows 2000 book also includes excellent additional information.

When you think you have you server as you want it, run "`netstat -a >> c:\portsopen.txt`" at a command prompt to see which ports are open on the server.

3.2.2 IIS5

Ensure that when you install IIS5 (whether that is at the time of the Windows 2000 installation or afterwards) that you only install the parts you require. It is better to install too little initially and then add on what you require rather than add

all, then remove parts. Do not install the HTML manager and only install the FTP, SMTP and NNTP services if you really need them [6].

Microsoft have produced a IIS 5.0 Baseline Security Checklist which can be found at http://www.microsoft.com/technet/security/tools/chklist/iis5cl.asp and a Secure Internet Information Services 5 Checklist which can be found at http://www.microsoft.com/technet/security/tools/chklist/iis5chk.asp.

3.2.3 SQL Server 2000

Port 1433 for SQL Server appears consistently in the most attacked statistics, frequently just behind port 80 (http) [1]. This further emphasises the need to ensure that your SQL Server is secured – attacks would not be attempted if there were no possibility of success.

The first thing you need to ensure is that the sa account (the SQL Administrator) has a password set, and this should be a "strong" password that is not easily guessed (e.g. don't set it to be 'password'!).

Microsoft have a number of Technet articles concerning SQL Server 2000 and security including 'Make Your SQL Servers Less Vulnerable' (http://www.microsoft.com/technet/security/tools/chklist/sqlsec.asp), *SQL Server 2000 Security* (http://www.microsoft.com/technet/prodtechnol/sql/maintain/security/sql2ksec.asp) and 'SQL Server 2000 C2 Administrator's and User's Security Guide' (http://www.microsoft.com/technet/prodtechnol/sql/maintain/security/sqlc2.asp).

Another useful resource 'SQL Server Security Alerts and Information' can be found at http://www.swynk.com/friends/sjones/Alerts.asp.

3.2.4 Frontpage Server Extensions

There are some built-in functions to restrict access to STS web sites. Anonymous browsing can be disabled and only users who have been specifically allowed can access sites. Permissions are role-based, allowing users particular freedom within the site dependant upon the role they are assigned (e.g. administrator, contributor, browser). If a secure area is required a subweb can be setup with more restricted access than the site as a whole [7].

3.3 Additional Options

3.3.1 Firewall

For any connection to the Internet a Firewall should be your first point of security. Many people consider the NT4 platform to be particularly insecure because of

the number of ports the operating system has open and also due to the nature of those ports (such as NetBIOS), yet the Windows 2000 server platform has more open ports and active services than Windows NT [8]. STS when installed on this platform then adds a number of additional services (and open ports) that could be utilised by an attacker. A Firewall should be used to restrict access to only the ports required for the service to operate which would be port 80 (http) or port 443 (https) inbound and port 25 (smtp) outbound.

When using a Firewall you should place the STS server in a De-Militarized Zone (DMZ) so that should your server be compromised, it cannot be used as a staging point to attack your internal network. Access should be restricted through the Firewall from the Internal network to the DMZ, opening only the necessary ports – port 80 (http), port 443 (https) if your STS site requires it for either access, authoring (adding documents or other items) or administrating, port 1433 if you want to use SQL Enterprise Manager to remotely administer the database and perhaps a port for remote access to the Operating System (eg Terminal Services (port 3389) or PCAnywhere (port 5631)).

3.3.2 SSL

Using an SSL connection to your web server allows traffic between the client and the server to travel encrypted. As authentication is generally used to restrict access to STS sites, this will protect usernames and passwords. Additionally, any data transferred will also be protected.

It is possible to activate settings within STS that force an SSL connection to be used for particular situations. One sets a requirement for an SSL connection to be used for any administrative procedures the other sets a requirement for an SSL connection to be used for authoring.

3.3.3 Available Tools

- HFNetChk

HFNetChk was developed with Shavlik Technologies and free versions are available for download, HFNetChk from Microsoft and HFNetChkLT from Shavlik (http://www.shavlik.com/security/prod_hf.asp). In addition Shavlik have produced a more fully featured version call HFNetChkPro.

The basic function of this product is to analyze servers to see if they have the most recent patches applied to them. HFNetChk will read information on the server (usually values from the registry or the version number of an executable or DLL) and compare it to the latest patch list (which is downloaded from Microsoft). This does, however, require connectivity to the Internet to download the latest information.

The commercial versions that Shavlik have released differ from the version downloadable from Microsoft by including the ability to "push" patches to servers, while HFNetChkPro also has a built in file validation to ensure that patches have been installed correctly.

- Microsoft Baseline Security Analyzer (MBSA)

MBSA (developed with Shavlik Technologies) is available as a free download from Microsoft® (http://www.microsoft.com/technet/security/tools/Tools/MBSAhome.asp) and can be used to scan servers to see whether patching is up-to-date and if there are any gaping holes in the security of a server. MBSA combines the patch scanning of HFNetChk with additional scanning of the configurations and settings of the OS and of the Group Policy Objects to check how secure they are [9]. James Michael Stewart notes, however that "This tool should be used as a time saver and not as a replacement for solid security practices and an enforced organizational security policy". [9]

A commercial version of this tool (EnterpriseInspector) is available from Shavlik (see http://www.shavlik.com/security/prod_ei2.asp). EnterpriseInspector has been designed to be an enterprise version of the product. It enhances MBSA, using a database backend to store all the information gathered and allows you to generate custom reports.

- IIS Lockdown Tool

This tool is available as a free download from Microsoft® (http://www.microsoft.com/Downloads/Release.asp?ReleaseID=33961). It works by using templates that allow an administrator to easily turn off features that are not required for their particular IIS server.

As with any tool that you use, care should be taken when configuring the lockdown tool as you could end up breaking STS. The Administration FAQ document available at http://sharepointtips.com explains one such issue (although it refers to the tool incorrectly) where a search was returning a 404 (File Not Found) page. "This is usually caused by an IISLockup which has been run in default mode. This causes the executable path for .idq files (and others) to be changed to 404.dll leading to the automatic 404 error when the system tries to search". [10]

- URLScan

This tool is available as a free download from Microsoft® and will check the URL (Uniform Resource Locator, such as http://www.sans.org) of any connection that is established to the web server. By using parameters you set, it will block attempts made to use, for instance overly long URLs, which could be an attempt

to try and find or use an exploit in IIS that would then allow an attacker to access something on the web server that they should not.

There is a "HOW TO:" knowledge base article (Q318290) on installing the URLScan utility onto a server running STS because if installed in its default configuration the URLScan program is likely to "break" STS [11]. This article can be found at http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q318290.

This tool has been integrated into the IIS Lockdown tool (see above).

- SecureIIS

This tool was developed by eEye Digital Security. It is described as an application firewall and intercepts traffic bound for the web server and checks it before allowing it to be passed to IIS for processing provided it is not deemed to be a possible attack. Two of the possible attacks that the software looks for are buffer overflows and Parser Evasion Attacks. A buffer overflow attack is where the attacker tries typing in a URL that is longer than IIS is expecting (does not fit into the "memory space" (buffer) which has been allocated for this purpose). This could allow the attacker to execute any program of the attackers choosing on the web server (and quite possibly with administrative permissions). Parser Evasion Attacks try to use special characters in the URL to fool IIS. "Insecure string parsing can allow attackers to remotely execute commands on the machine running the web server. SecureIIS checks for various characters in a string that would allow an attacker to add on commands to a normal value". [12]

Further information on this product can be found at http://www.eeye.com/html/Products/SecureIIS/index.html.

- Applock/Web

This tool was developed by WatchGuard Technologies Inc. and is intended to protect web content and IIS application by intercepting requests and blocking those that are deemed to be attacks. It is also designed to protect the Operating System, acting at the kernel level (running as a device driver).

Further information can be found at http://www.watchguard.com/products/applock.asp

- Entercept Web Server Edition

The Entercept WSE tool was developed by ClickNet Software and is designed to protect web servers by "evaluating requests to the Web server, the application programming interface (API), and the operating system, before they are processed" [13].

Further information on this product can be found at
http://www.clicknet.com/products/wse/

3.3.4 “Split Infrastructure”

Whilst STS can be run on a single box, this means running multiple services on one server and consequently opens more possibilities for attack, either direct or via “proxy” (for example “attack” the local database or file system using an IIS security hole).

- Mail Server

Putting an additional server to handle all mail (which will be outbound only) will restrict direct traffic between the STS server and the Internet. (It will also become a useful central point if you should end up with a number of STS servers).

It would also be advisable to use a product such as MAILSweeper (http://www.mailsweeper.com), which can be used to ensure that no viruses are being sent out (a sure way to upset your clients!) and also for its content scanning capability should you feel it necessary. You may of course already have a server in place for your day-to-day e-mail traffic.

- SQL Server

Putting the SQL server onto a separate server will limit its exposure to the Internet. Frequently attackers will use the vulnerability in another program (eg IIS) to allow them to run commands and/or programs to attack their true target. If the SQL Server programs are on the web server for instance and installed in the default location the attacker could use an IIS exploit to try and access a SQL program and/or the database directly.

3.3.5 Reverse Proxy

A proxy server “acts as an intermediary between a Web client and a Web server” [14]. It is normally used on a network to accept requests from internal clients and redirect their web server requests externally, allowing a single IP address to be used for external access and adding security by separating the clients from direct access to the Internet.

In contrast a “Reverse Proxy” server is used to proxy web requests inbound from clients (or proxy servers) to the web server. This gives an added layer of security by separating the web server from the Internet as the inbound network connection is terminated at the “Reverse Proxy” and a new connection opened from there to the web server.

4. Closing Thoughts

Any web server that is put on a network (especially the Internet) must be considered vulnerable, and System Administrators should use whatever information and tools that are available in order to leave the smallest possible opening on their systems for a hacker to exploit.

Using any of the techniques described above on their own will not give you a robust and secure solution, e.g. “patching systems is not a perfect security solution” (Ferrairo & Mell) [4], “Firewalls alone don't provide adequate defences, particularly against something like Code Red” [15]. The effectiveness of the solution you decide on will depend upon how you use the various tools available and the procedures you put in place for dealing with required updates, such as patches. No solution will be entirely secure – the aim is to reduce the risk. As Marcus Ranum explains in his Foreword to the First Edition of the book Hacking Exposed “Most of the hacking being done is using simple tools that scan entire networks for "low hanging fruit" – easy targets with weak defenses. Shoring up those basic weaknesses can make the difference between your being a statistic or being bypassed by the bad guys as too tough a nut to crack” [16].

What does the future hold for STS? Well, Paul Krill of InfoWorld reveals the following; “To be built on top of the Microsoft .Net Framework programming model and shipping in mid-2003, SharePoint Team Services 2.0 will first be released as a separate add-on and then be included with the operating system itself” [17]. This will of course bring new security issues with it, but that’s for another time.

List of References

[1] “InternetStormCenter: Top 10 Ports”
http://isc.incidents.org/top10.html

[2] Lemos, Robert “DDoS attacks - one year later”
7 February 2001
http://news.zdnet.co.uk/story/0,,t269-s2084263,00.html

[3] “STS Overview”
http://www.microsoft.com/technet/prodtechnol/sharepnt/proddocs/spdocs/enduser/wscTSite.asp

[4] Ferraiolo, Dave & Mell, Peter “Operating System Security: Adding to the Arsenal of Security Techniques”
http://csrc.nist.gov/staff/mell/dec99-bulletin.pdf

[5] Semilof, Margie “Microsoft to clarify language on patches, fixes and updates”
11 September 2002
http://searchwin2000.techtarget.com/originalContent/0,289142,sid1_gci850374,00.html?Exclusive=True

[6] Cooper, Russ “10 Steps to Better IIS Security”
August 2001
http://www.infosecuritymag.com/articles/september01/features_IIS_security.shtml

[7] Burk, Mary “Frontpage Security Best Practices”
June 2002
http://msdn.microsoft.com/library/en-us/dnfp2k2/html/WP1_0602.asp

[8] Stewart, James Michael “Vulnerable ports on Windows 2000 Web servers”
5 February 2002
http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci800125,00.html?FromTaxonomy=%2Fpr%2F282598

[9] Stewart, James Michael “MBSA can help protect your Web server”
7 May 2002
http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci821736,00.html

[10] Walsh, Mike “Administration FAQ (unofficial)”
21 August 2002 (continually updated)
http://www.sharepointtips.com

[11] “HOW TO: Use URLScan with FrontPage 2002”
13 February 2002
http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q318290

[12] “SecureIIS Application Firewall: Proactive Web Server Security”
2002
http://www.eeye.com/html/Assets/pdf/siisDataSheetLowRes.pdf

[13] “Entercept Web Server Edition”
http://www.clicknet.com/products/wse/

[14] “NetLingo Dictionary of Internet Words A Glossary of Online Jargon with Definitions of Terminology & Acronyms”
http://www.netlingo.com/inframes.cfm

[15] Leyden, John “Security patch approach is failing”
23 July 2001

http://www.theregister.co.uk/content/archive/20564.html

[16] Ranum, Marcus “Hacking Exposed: Foreword to the First Edition” http://www.hackingexposed.com/Foreword/foreword1.html

[17] Krill, Paul “Microsoft readies SharePoint 2.0 collaboration platform” 6 September 2002 http://www.infoworld.com/articles/hn/xml/02/09/06/020906hnsharepoint.xml