Global Information Assurance Certification Paper

Microsoft IIS 6, Secure by default? How to Take Precautions.

Balal Ahmed
06 July 2003

GIAC Security Essentials Certification (GSEC) Practical Assignment
Version 1.4b Option 1- Research on Topics in Information Security

Abstract: -

Microsoft has received bad press for its products being inherently insecure. This has affected its standing in the marketplace. Several high profile vulnerabilities have allowed IIS servers to be hacked. To remedy this Microsoft have adopted new initiatives and have attempted to help end users by distributing advice and free tools.

This paper looks at the positive steps Microsoft have taken to help users of IIS and how the “Trustworthy Computing” initiative has shaped the security of IIS 6.0. New features are highlighted, as are some installation precautions. A section on practical steps that can be taken to further secure IIS 6.0 is included. The paper concludes with a short discussion on how to prepare for an intrusion

Table of contents

ABSTRACT: - 2

1.0 INTRODUCTION:- 4

1.1 TRUSTWORTHY COMPUTING IS THE GOAL 5

2.0 WHAT'S NEW IN IIS 6.0 6

3.0 SECURING IIS 6.0 7

3.1 SOME GENERAL ISSUES BEFORE STARTING 7

3.1.1 Policy 8

3.1.2 The three P's 8

3.1.3 Physical security 8

3.1.4 Secure the network 8

3.1.5 Harden the foundation 8

3.1.6 IDS and IPS 9

3.1.7 Upgrading from IIS 5.0 9

3.2 SOME PRACTICAL STEPS:- 9

3.2.1 Disable IIS in Active Directory global policy 9

3.2.2 Installation path 9

3.2.3 Disable services that are not needed 10

3.2.4 Securing the Metabase 10

3.2.5 Delete the default website 11

3.2.6 Configure custom error pages 11

3.2.7 Anonymous access 11

3.2.8 Logging 11

3.2.9 Worker processes 13

3.2.10 Use Encryption 14

3.2.11 ISAPI Extensions 15

3.2.12 Mime Types 16

3.2.13 Patching 16

3.2.14 Use ACL Authentication 16

3.3 SMTP SERVICE 16

3.3.1 Tying down the SMTP service 17

3.4 THE FTP AND POP3 SERVICES 17

3.5 THIRD PARTY UTILITIES 17

4.0 IF THINGS GO WRONG 18

5.0 CONCLUSION 19

6.0 REFERENCES 19

7.0 BIBLIOGRAPHY 21

1.0 Introduction:-

"We really haven't done everything we could to protect our customers ... Our products just aren't engineered for security"

"Every operating system out there is about equal in the number of vulnerabilities reported, we all suck."

Brian Valentine, Senior Vice President of the Windows Division, 05/09/02 [1]

Back when Microsoft was marketing Windows NT 3.5 as a secure operating system, the “internet” was primarily an educational resource. Educational and Government organisations were Internet enabled but most consumers and corporations had not started to realise the potential this global public network had to offer. Microsoft had not then started shipping a web server with the base product. The EMWACS web server (third party) was provided as part of the resource kit [2] and offered basic functionality.

The commercialisation and proliferation of the web resulted in the Internet Information Server product being shipped as an option pack to the core of Windows NT 4.0 operating systems. The first IIS server to gain widespread acceptance was IIS3

According to the Netcraft survey, Microsoft Internet Information Server started gaining public deployment in early 1996 [3] and currently holds approximately 25 percent of the web server market with a peak of 30% in mid 2000.

IIS was particularly successful during the dot com boom. Rapid deployment and ease of scripting helped in gaining market share. IIS has been losing market share since October 2002, primarily to Apache. The primary cause for this can be attributed to the reputation for security flaws allowing the confidentiality, integrity and availability of systems running IIS to be compromised. This gave IIS the reputation of being “inherently insecure” [4]

Microsoft’s strategy was to make IIS:-

- *Free:*- It was bundled as part of the Operating system or available for free download as an option pack.
- *Feature rich*:- IIS provided support for several Microsoft based scripting languages (Vbscript/ASP)
- *Extensible*:- Through the ISAPI module, third parties could add functionality for example Coldfusion, Perl and PHP

---

[1] Brian Valentine, SVP Windows division

.[4] Atrax, Basic IIS security precautions

- Easy to use:- Maximum features were enabled out of the box.
- Deployable:- Installed as part of the base OS (Windows 2000) and enabled as a running service by default.

Practically this was achieved by enabling maximum functionality, samples and scripts when installed as default. In the case of IIS5 the product was installed as part of the host operating system, Windows 2000 server, and enabled to start at boot by default.

All IIS versions have been feature rich and provide functionality that many organisations have found invaluable. While the features list is impressive the security track record has not been as notable. Consequentially IIS has been a victim of its own success as many of the vulnerabilities present in IIS 3, IIS4 and IIS5 could have been mitigated by following simple hardening and patching methodology.

Current evidence would suggest that IIS has not been technically mature from a security perspective up to and including IIS 5. Microsoft seems to have taken this general feeling on board and launched an initiative to increase confidence in its products.

Microsoft claim to have rewritten IIS 6.0 from the ground up utilising new coding methodologies and discipline. There have been several security enhancements that claim to make IIS 6 “secure by default”. Functionality has also been broadened and enhanced. Does this then imply that a default installation is robust enough to be exposed to the harsh Internet?

1.1 Trustworthy Computing is the goal

There are no less than 70 advisories either directly or indirectly related to IIS published on the Computer Emergency Response Team (CERT) website [5]. The security considerations of installing an IIS system have haunted security managers and professionals alike. While IIS has received bad press for being insecure, many of the compromised hosts were not being used as web servers.

The default installation windows 2000 server included IIS 5. This led to many more servers running IIS than should have been. For many organisations rouge web servers were a problem particularly in development departments where unhardened development servers were particularly vulnerable. This led to an increased “attack surface area” and “attack depth”. The attack surface area was increased due to more servers running IIS as they had not been hardened. The attack depth was increased as a result of ISAPI extensions and sample scripts being left intact on unhardened web servers thus increasing attack modes and vectors.

These insecurities of Windows and IIS have been detrimental to Microsoft’s reputation, resulting in Microsoft being placed under extreme scrutiny. To

mitigate these certain steps were taken by Microsoft to help the user community to maintain and regain confidence in these products. These are summarised below

- The creation of www.microsoft.com/security:- A central URL for resources was invaluable for administrations. The URL was launched along with the undertaking that Microsoft would be open and honest regarding security. This URL remains a central point for researching vendor related patch information.
- Security Bulletins: - email bulletins and notifications were initiated
- Acknowledgements: - Microsoft would acknowledge the individual or establishment for finding and alerting them [6] about vulnerabilities.
- IISlockdown tool: - a tool that reduces the attack depth by removing selected components from the configuration.
- Baseline security analyser and hfsnetchk:- A tool that analyses vulnerability levels and advises the administrator on what patches are missing [7].
- Windows update: - an online tool that checks for patch levels and automates downloading and installation. Windows Software Update service is the enterprise version of this service. An excellent detailed discussion is available by John Ives [8]
- Configuration guides that provide best practice guides [9]

The response capabilities of Microsoft have evolved; customers now seem to trust that once a vulnerability is escalated, Microsoft will deploy a patch as soon as possible [10].

To further assure customers and the user community, Bill Gates launched the "Trustworthy Computing" initiative. What is trustworthy computing? It is an ethos that drives the various people involved in a system to design, build, deliver and maintain a robust system.

This ethos is at the very heart of the Microsoft security development plan [11]. This means that an application will be built from the ground up with this initiative in the fore. This translates to secure by design, secure by build, secure in deployment and secure in run scenarios. It is common knowledge that Bill Gates ordered every developer in Microsoft to undergo security training [12]. The first major product to benefit from this initiative was to be the Windows 2003 server suite of products. IIS 6.0 has also undergone a similar process and it is claimed has benefited form the trustworthy computing initiative.

2.0 What's new in IIS 6.0

IIS 6.0 has undergone a major overhaul from IIS 5.0. Certain architecture changes have been made to increase availability. Worker process and process recycling achieve this. Runaway processes are now automatically

recycled to keep web sites up and running without affecting other components.

An Improved management Interface has been designed. Any systems administrators that have had to write automation scripts to automate certain tasks in IIS 5 would be familiar with the IIS Metabase and the difficulty in editing it. The Metabase has now been changed to an XML editable file. Changes can be made on the fly without having to restart services. While this may ease administration, it may also have an adverse effect on the confidentiality of the system, particularly if the XML file is compromised.

IIS 6.0 is locked down by default. It now is an installable option that needs to be initiated by a user with administrative privileges. It is no longer installed as part of the base operating system. Installing IIS 6.0 does not increase the deployment time by much but does remove the issue of rouge or unwanted web servers that were installed “by accident”. User level security has also been improved with improved authentication and authorisation.

IIS 6.0 to a certain extent now also has the ability to mitigate web based DoS attacks. This feature is known as rapid fail protection. If a particular web application is being attacked and fails repeatedly, IIS 6.0 will remove this process completely to maintain the availability of the remaining applications. A trap can be sent to an administrator or the server can be shutdown thus taking it out of a high availability cluster.

Extensions lockdown: - Out of the box there are no dynamic content extensions configured. The server can only serve static content until an application handler is registered on the system. By taking this approach Microsoft have laid responsibility clearly at the feet of the web server administrator to ensure the application extension that is being registered is valid.

Worker process privilege:- The worker process threads operate under the context of a low privileged account, this is either equivalent to the anonymous user privilege or another low privilege account. If a worker process is compromised the damage that can be inflicted as that user will be minimal.

3.0 Securing IIS 6.0

IIS 6.0 was designed for use on windows 2003 server & is distributed as part of the core operating system at no extra cost. The following discussion does not encompass the hardening of the base operating system.

3.1 Some general issues before starting

There are several precursors to installing any IT related equipment or service. The exact procedures will depend on the organisations policies and practices. A brief summary of these is provided below.

3.1.1 Policy

It may sound like a cliché but the point cannot be emphasised enough

“Refer to the security policy before installing, configuring and deploying services”

It is crucial to consult the relevant issue specific policies before even considering installing any software, be it the Operating system or the web server software. If issue specific policies do not exist, then formulate them! Many issues arise due to a lack of a coherent policy relating to web servers and services. Resources are available freely on the Internet to aid security practitioners and managers to author policy.

3.1.2 The three P’s

Plan, plan and plan. A successful installation that meets the objectives defined depends on a clear understating of the steps required to achieve those objectives. This is even more important for IIS web servers. A well-structured plan will highlight all the relevant steps; highlight risks and corrective action to be taken at each step. A documented record of how certain risks have been mitigated along the project timeline could be invaluable if a forensic analysis is needed in the future.

3.1.3 Physical security

“There is no security without physical security” [13]

While this may seem obvious, it is often overlooked, particularly in the case of development machines. Access control should be used where appropriate to validate and log staff and visitor access to secure areas. Ensure the physical environment is suited to host the equipment, including power, environmental control & monitoring

3.1.4 Secure the network

Network layer considerations should be thought through in detail. Packet filtering should be performed on border devices such as routers. web servers should be placed behind firewalls, utilising both ingress and egress filtering where possible. The exact placement needs to be determined relative to the value of data being served by the web server. For intranet servers it may be prudent to place these in a three-tiered architecture. Logs of traffic to and from the web servers should be collected and retained for analysis in the event of a breach.

3.1.5 Harden the foundation

IIS 6.0 runs on the Windows 2003 server series. To ensure the security of IIS 6.0 it is essential that the base operating system be hardened. The installation

and hardening procedure may differ from, say a file and print server, so it is again prudent to refer to the issue specific policy.

As of writing, Windows 2003 has been on general release for approximately 2 months. As such third party documentation (Checklists) on hardening the OS are not widely available on the Internet. There is a need for such checklists to be formulated, and it is envisaged that these will become available as time progresses.

The server should not be connected to the network until hardening has been carried out.

3.1.6 IDS and IPS

Intrusion detection systems have matured significantly in recent years. The commercialisation of this corner of the market has led to manageable products with signature updates. The open source community has also been growing strongly. An IDS is key in detecting potential attacks. Network and host based IDS / IPS should be deployed to warn of attacks. Heuristics based appliances can also filter URL's for known attack strings such as the directory traversal and code red strings. Filtering these upstream from the server will reduce the possibility of the attack reaching the server.

3.1.7 Upgrading from IIS 5.0

Out of the box IIS 6.0 is locked down. Many components are not installed, however when upgrading from an older version settings and components are retained. A clean installation of IIS 6.0 should be performed and services migrated over from the older version.

3.2 Some practical steps:-

The following discussion is not intended to be an exhaustive discussion on all configurable options under IIS 6.0. Every installation will be individual in its requirements and configuration.

3.2.1 Disable IIS in Active Directory global policy

Group policy now offers a property to control which servers can install and run IIS. Use Group policy to restrict installation rights to preauthorised computers and administrators. These rights should not be given to a generic account but to a group, and by adding permitted administrators to this group.

3.2.2 Installation path

The web root should be placed on a separate partition to the core operating system. A partition formatted with NTFS, while not essential is strongly recommended. Whilst installing IIS 6.0 care should be taken to ensure the default installation path is changed as appropriate. File permissions to secure

content should be applied. Appling “no access” ACL’s to files that should not be served to anonymous users will prevent accidentally publishing content that should not be served anonymously.

3.2.3 Disable services that are not needed

IIS 6.0 consists of six components, namely, IISadmin, FTP publishing service, POP3 service, SMTP service, HTTP SSL and the www publishing service. If any of these components are not required for the web server to fulfil its role, they should be disabled from the services applet in the control panel. The exception to this is the IIS admin service as it is needed to run other IIS services, hence should not be disabled.

3.2.4 Securing the Metabase

The IIS 6.0 Metabase has been completely reworked from its predecessor. While the function remains the same, namely to store configuration data pertinent to IIS, the format has changed. The Metabase is now an XML file that can be edited using editing tools such as notepad.

IIS 6.0 now has the ability to immediately apply any changes made to the Metabase as soon as the file is saved. This is a configurable option on the global properties of the web server or by editing the Metabase as below

```
IIsComputer Location ="/LM"
    EnableEditWhileRunning="0"
    EnableHistory="1"
    MaxBandwidth="4294967295"
    MaxHistoryFiles="10"
IIsComputer
```

To enable this feature edit this property to a value of “1” and restart IIS.

While this feature allows automation of changes it also leaves the server vulnerable to defacement and attack.

Do not enable the “edit while running” property unless there is sound justification for doing so. If this must be enabled an appropriate risk analysis must be conducted.

IIS automatically keeps a history of previous configurations to aid recovery and roll back. By default the last ten configuration changes are kept. The number of backups kept is configurable via the “MaxHistoryFiles” directive in the Metabase. It is advisable to increase this number based on available disk space. By default the history files are located in the %system root%/system32/inetsrv/history directory. This directory should be secured as described below

The Metabase holds a wealth of information about the configuration of the web server. An attacker would gain invaluable information about the web server by obtaining this file. By default only the local system and the built in administrators group has access to the Metabase and the automatic backups. This should be changed by removing the builtin administrators group and adding in specific users.

3.2.5 Delete the default website

Even though IIS 6.0 is locked down out of the box the default website should be deleted. Several UDDI aspx samples are configured on the default site and it is better to start with a clean website container.

3.2.6 Configure custom error pages

Web server error pages feed back information to the user when an error occurs. The most common of these errors is the well known '404' page not found error.

While the default pages will server up error pages for the standard error codes it is advisable to rewrite these, customised for your website.

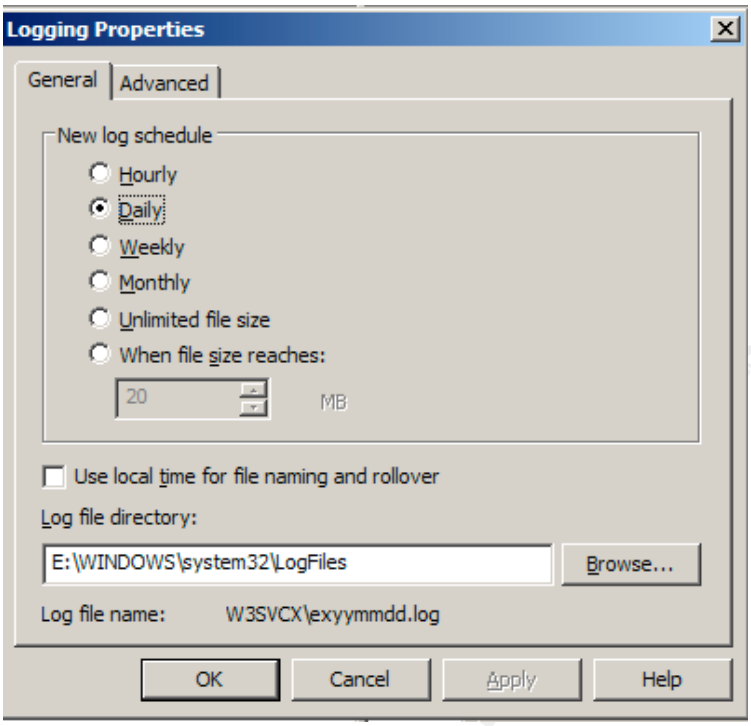
3.2.7 Anonymous access

Many web servers will serve content to anonymous users. This mode of access allows untrusted users to access content while masquerading as a specific user configured on the server. By default IIS 6.0 still uses the IUSR_computername account to grant access to anonymous users. NTFS file level permissions and web server directory ACL's should be used to provide two layers of security while accessing content. Write access should be denied for this account.

A specific "Deny all permissions" ACL should be applied to all files that do not need to be served anonymously.

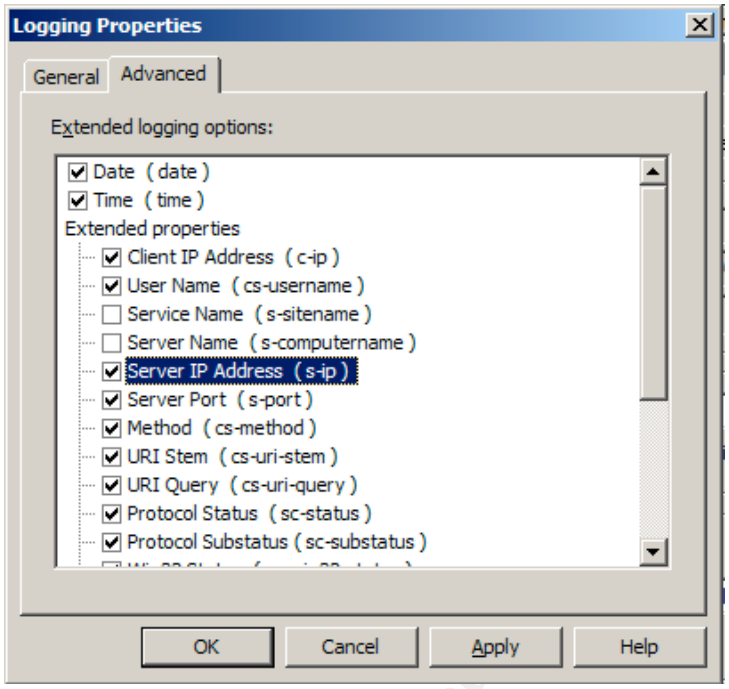
3.2.8 Logging

High quality logs are an essential component of a defence in depth policy. Whilst logs can provide excellent traffic and capacity planning for services, they can also prove invaluable during a forensic analysis. The correct level of logging needs to be selected. IIS provides several logging formats. The W3C extended logging format is recommended as this allows logging of extended HTTP header information.



The above screen grab depicts the W3C extended logging properties page for the default IIS website. The log rotation scheme should be chosen on the amount of requests being severd by the server. Web logs can be large so ensure that disk size checking is performed on the drive where the logs are held.

The advanced properties page allows extended fields to be logged. The level of extended logging should be selected based on the sensitivity of the data served.



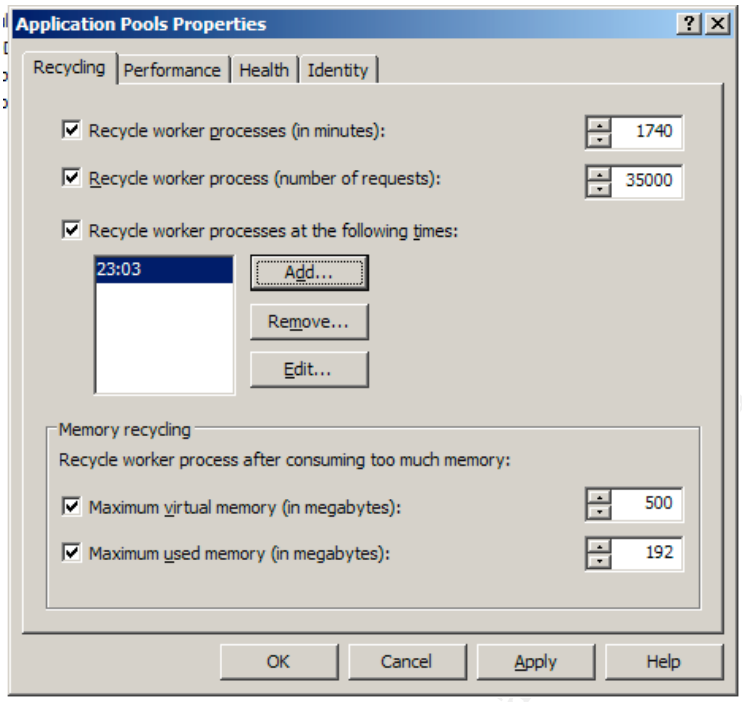
Build application level logging into web applications. If possible the security officer should be consulted during the coding and building of such applications. Developers traditionally use application logging for troubleshooting; this concept should be expanded to authentication, auditing and authorisation.

3.2.9 Worker processes

IIS 6.0 can operate in “worker process isolation mode” or “IIS 5.0 isolation mode”. This facilitates backwards compatibility for older applications that need to share a single process.

Worker process isolation mode is strongly recommended. Web application pools can be configured to serve dynamic content securely. Worker processes now automatically check for buffer overflows and can shutdown and respawn unruly processes.

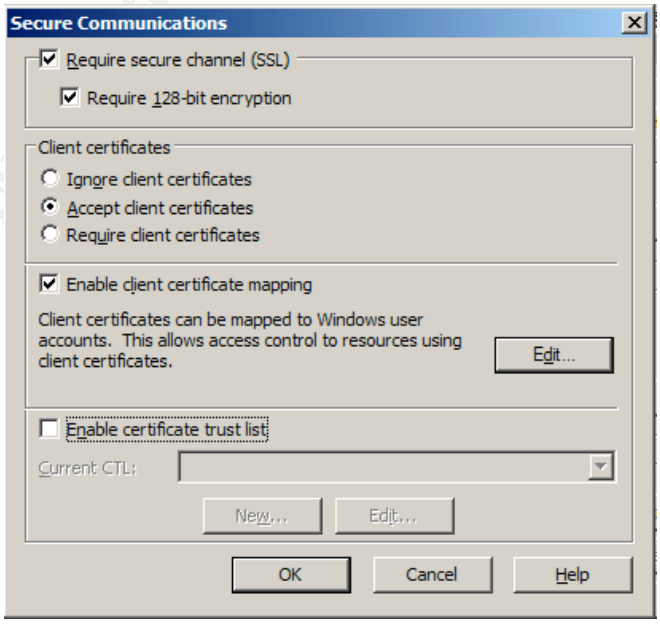
Applications that keep failing can be rapidly restarted to prevent DoS attacks.



Specifying memory usage limits can help to keep runaway processes under control

3.2.10 Use Encryption

SSL technology is well matured and has been the primary technology that has brought confidence to Internet based transactions. Data is encrypted from the client to the server, thus preventing eavesdropping and compromising sensitive information such as personal details and credit card numbers. SSL should be used where appropriate to encrypt the web experience.



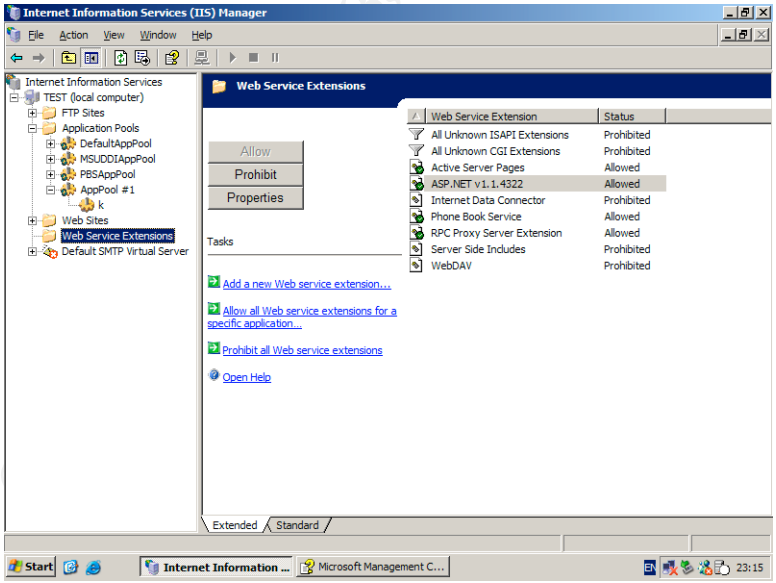
Before SSL can be used a valid Certificate must be obtained from a certificate issuing authority such as Verisign. A certificate-signing request (CSR) needs to be generated on the web server. This CSR is password protected. A strong password should be chosen. Care must be taken as once the password is lost the CSR cannot be used until it is revoked.

When choosing a Certificate authority (CA) to sign your CSR shortlist only reputable companies. An SSL that has been authorised by a public CA is visible to all users and apart from being used to encrypt data is also used to validate the identity of the organisation trading on the web. A low quality CA may adversely impact the image and reputation of the website.

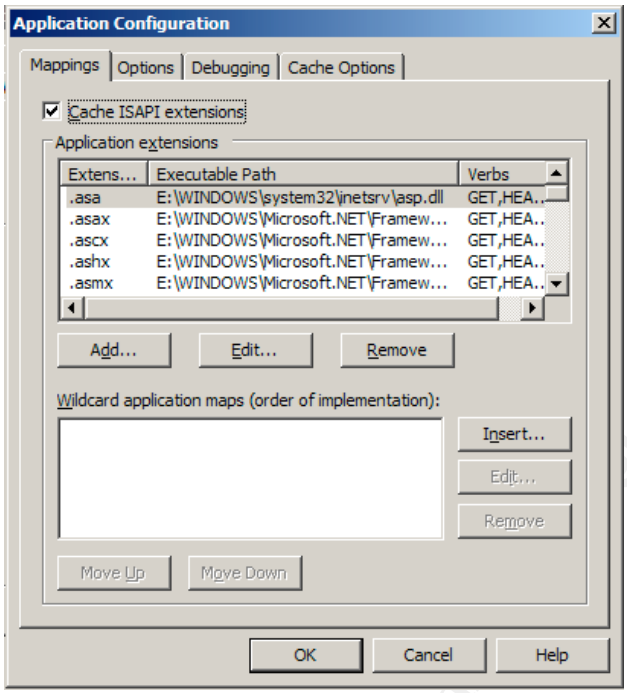
Client certificates can be used in place of the traditional username and password authentication model. While this is significantly better, it does demand high management overhead in order to distribute and maintain client certificates. The CA used to sign certificates must also conform to widely accepted procedures. In general client side certificates are useful in intranet, partner net and extranet deployment scenarios

3.2.11 ISAPI Extensions

ISAPI extensions are now created and controlled from the web service extensions branch. This is a central point where all extensions can be validated and authorised.



Ensure that only required ISAPI filters that are needed are configured on individual virtual directories. This is performed from the directory application configuration applet as shown below.



3.2.12 Mime Types

Mime types tell the web server how to deal with files with particular extensions. Out of the box IIS 6.0 comes preconfgiured with an extensive list of extensions. Only extensions that are being served should be configured. The list can be edited from the global properties page or directly in the Metabase

3.2.13 Patching

Much of the damage that the Slammer, code red and Nimda worms done were as a result of a vulnerability that had previously been patched by Microsoft. To maintain a secure server it is essential to patch any new vulnerabilities that are discovered. Patches should be tested in a lab or test environment before deployment to live servers. Tools such as Software Update Server/Windows update may however be used to aid deployment of patches.

3.2.14 Use ACL Authentication

IP packet filtering will be applied at the network level using firewalls or routers. A true defence in depth policy will also apply these same controls at the application level. IIS offers the facility to perform IP address authentication. This is particularly useful in intranet and extranet scenarios

3.3 SMTP service

The SMTP service is used to send email out to users, posted from web applications. A typical example is automated subscription emails sent from a web site. The service also has the ability to function as a full SMTP relay agent, forwarding email on behalf of other hosts.

3.3.1 Tying down the SMTP service

By default the SMTP service binds to all unassigned addresses. If the server has multiple addresses that are in use for different services this should be tied down to the relevant IP address.

Use IP based connection control ACL's to validate hosts that are to be permitted to relay through the server. This will prevent open relay and spamming potential

Only servers and domains that are allowed to relay should be permitted in the relay configuration. Open relays are a significant issue on the internet and can be used for spaming.

Logging is turned off by default. Turn this on and use the W3C Extended log file format to collect data.

Monitor the badmail directory for potential spamming behaviour. Spammers often send bulk emails to a large list of users. Check the badmail directory and check if email that has not been sent should have originated at the web server. The default path of the badmail directory is c:/inetpub/mailroot/badmail

3.4 The FTP and POP3 services

The hardening of these services is not discussed in this document. This is an area upon which future GSEC candidates could expand on.

3.5 Third party utilities

Utilities such as SecureIIS can be used to improve security [14]. Often vendor claims need to be validated against each individual situation. Third party utilities can enrich the base product. At the time of writing these are limited due to the recent release of windows 2003. As time progresses new tools that enhance security are expected to become available

3.6 Perform Operational Readiness testing

To maintain consistency an operational readiness and deployment test should be formulated. This is to ensure that any set procedures and policies have been adhered to and that the build complies with a minimum standard.

Vulnerability assessment tests should be conducted against new servers. This can be automated and managed by using specialised tools such as nessus [15] and retina [16].

Service availability and assurance should be tested using stress-testing scripts to ensure the availability aspect does not suffer. While this is generally the remit of server management teams, the availability factor is often built in to security policies due to DoS attack issues. If appropriate a simulated DoS attack should also be factored in to the Opertational Readiness Testing regime.

Setting up a structured test checklist and peer audit review of any builds will ensure that all mitigating measures have been applied.

4.0 If things go wrong

Taking precautions and monitoring is part of the picture. Hardening servers, while reducing the chances of being compromised, does not unfortunately eliminate this possibility. The approach one should take is, “what will we do if we get hacked”

The worst time to put together a process is AFTER an event has taken place. Define a policy that deals with the action plan that needs to be followed if a server is compromised. This may include

- Management escalation procedures:- Who should be informed and under what circumstances. For example at what point should the CEO be informed of an intrusion? At what point is the Technical director to be informed? Do management need to be advised if a minor hack attempt is attempted from the inside of the network etc.
- Coordination duties:- Who is to record actions taken and follow actions vs a timeline of events. Who will co-ordinate the various teams and organise emergency meetings
- Technical escalation:- Which teams have the remit to initiate the Incident handling procedures. Who is responsible for preserving the evidence?
- data recovery:- Who has the authority to invoke the backup and restore procedure? How will the evidence be preserved if the system is wiped & restored form a good backup
- Invoking contingency & continuity plans:- When will the live service be switched over to a backup facility? How will this be initiated and who has the authority to authorise this.
- Forensics and post mortem analysis. How is this to be handled, what is the objective of such an activity. Who should be advised of the results and how will the event be prevented in the future?

A clear-cut incident handling procedure is needed to efficiently manage an event such as a web server hack. The author was involved in dealing with a major incident that caused an entire web farm to be taken off line for five hours due to an intrusion on two IIS servers. At the time there were no clear-cut processes or procedures for dealing with intrusions. Lack of containment

procedures led to the dramatic decision to take the entire web farm off line. This affected forty servers and approximately 250 clients. As a result the web farm was taken off line for longer than was technically necessary while management were engaged in a discussion about whom could authorise bringing the data centre back on line.

Such errors can be avoided by putting in place guidelines on how to deal with scenarios that may occur. A scenario plan for each element of the security policy can be drafted up and archived for use if needed. An example could be how to deal with a disgruntled employee severing network cables before leaving or a failure of a set of UPS devices and the power failing at the same time.

5.0 Conclusion

Microsoft has made significant advances in securing IIS 6.0. The Trustworthy computing initiative appears to have had an effect on the default installation of IIS. This in itself is not enough to keep a server secure. A Defence in depth approach, when applied to a default configuration of IIS shows that many steps can be taken to lockdown potential intrusion vectors. Taking proper precautions and applying the fundamentals of IT security to IIS 6.0 will further enhance the security.

Microsoft has taken a step in the right direction, however only time will tell whether these measures have been effective. It is too soon to validate if the quality of coding has improved or not.

6.0 References

1
http://archive.infoworld.com/articles/hn/xml/02/09/05/020905hnmssecure.xml
Lead Windows developer bugged by security
Matt Berger September 5, 2002 1:46 pm PT

2
http://www.simonstl.com/projects/tcpip/windownt/webinst.html
Installing a web server, Simon St.Laurent.1995

3
http://www.netcraft.com

4
Basic IIS security precautions
by : Atrax
http://www.readthefuckingmanual.co.uk/infinitemonkeys/articles/iis/992.asp

5
http://www.Cert.org

6
Acknowledgment Policy for Microsoft Security Bulletins
January 26, 2000
https://www.microsoft.com/technet/security/bulletin/policy.asp?frame=true

7
Baseline Security Analyzer White Paper
Microsoft Corporation, June, 2003
https://www.microsoft.com/technet/security/tools/tools/mbsawp.asp?frame=true#d

8
Using and evaluating Windows software update services
John Ives 2003
http://www.giac.org/practical/gsec/John_Ives_GSEC.pdf

9
Secure Internet Information Services 5 Checklist
29-June-2000, Michael Howard
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/iis5chk.asp

10
Gartner: Drop Microsoft IIS now
Wendy McAuliffe ZDNet (UK) September 24, 2001
http://zdnet.com.com/2100-1104-530757.html

11
Microsoft product briefing Info security London

12

The Journey to Trustworthy Computing: Microsoft Execs Report First-Year Progress
REDMOND, Wash., January 15, 2003
http://www.microsoft.com/presspass/features/2003/jan03/01-15twcanniversary.asp

13
March 13, 2003
No Security Without Physical Security
By Larry Seltzer
http://security.ziffdavis.com/article2/0,3973,930456,00.asp

14
http://www.eeye.com/html/Products/SecureIIS/

15
http://www.nessus.org/

16
http://www.eeye.com/html/Products/Retina/index.html

7.0 Bibliography

1
The World Wide Web Security FAQ
Lincoln D. Stein & John N. Stewart , February 4, 2002
http://www.w3.org/Security/Faq/

2
Beefing Up IIS: 10 Tips From A Former Solaris Admin
By: Matt Foley, Published: 21st Sep 2002
http://www.devarticles.com/art/1/207/2

3
Deploying Windows 2000 with IIS 5.0 for Dot Coms: Best Practices, White Paper
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/iis/iis5/deploy/depovg/iisdtcom.asp

4
http://www.sans.org/rr

5
http://www.securityfocus.com

6
http://www.jsiinc.com

7
http://www.iisfaq.com

8
IIS documentation
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/iiswelcome.asp

9
http://www.mcpmag.com/security

10
Microsoft's IIS6 lockdown

September 02, 2002
URL:

http://www.zdnet.com.au/builder/program/windows/story/0,2000035027,20267848,00.htm

Last Updated: July 26th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 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
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 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
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
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
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
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
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
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
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