CERT-In

Indian Computer Emergency Response Team

Enhancing Cyber Security in India

Securing IIS 6.0 Web Server

Department of Information Technology
Ministry of Communications and Information Technology
Govt. of India

Version: 1.0 **Issue Date: 11-10-2006**

Table of Contents

1. Introduction 4
2. Overview of IIS 6.0 5
   2.1 Salient Architectural Features of IIS 6.0 5

3. Host Security 8
4. Secure IIS Configuration 9
   4.1. Minimize Default Installation 9

      4.1.1 Essential IIS components & services 9
      4.1.2 Delete default sample files and websites 12
      4.1.3 Web Services Extensions 12
      4.1.4 Disable File System Object (FSO) Component 13
      4.1.5 Enable Only Essential MIME Types 13

   4.2. User Rights and Permissions 14

      4.2.1 IIS User Accounts 14
      4.2.2 Authentication 16
      4.2.3 Metabase Permissions 18
      4.2.4 Fine Tune Metabase Settings 19
      4.2.5 Securing IIS Website Permissions 20
      4.2.6 Securing the Web Site Directory and Content 21
      4.2.7 Setting IP Address and Domain Name Restrictions 22
      4.2.8 Isolating Applications 23
      4.2.9 Evaluating the effects of Impersonation on Application Compatibility 24
      4.2.10 Configure Web Sites and Applications for Isolation 24

   4.3. Other Security configurations 26

      4.3.1 Configure the custom error Pages 26
      4.3.2 Configuring Secure Sockets Layer 26
      4.3.3 Logging 27
      4.3.4 Backup 31
      4.3.5 Network Security 31
      4.3.6 Reviewing Security Policies, Processes & Procedures 32

5. Content management 35
   5.1 Front Page Extensions 35
   5.2 Security considerations for Content Management 35

6. Secure Coding 36
7. Security tools 37
8. References 38

Annexure-I 39

List of Tables

Table No.	Description	Page No.
1	Subcomponents of IIS	9
2	Subcomponents of WWW Service	11
3	Predefined Web Service Extensions	12
4	Comparison of Web Site Authentication Methods	18
5	IIS Metabase settings	20
6	Web Site Permissions that are supported by IIS 6.0	20
7	NTFS Permissions for different files	22
8	Log file fields	28
9	TCP and UDP ports associated services	31
10	Windows server 2003 Operating System security	33
11	Windows Server 2003 Policy security	33
12	Firewall and Router Security	33
13	Miscellaneous Security	34
14	Recommended Service startup types on a dedicated Windows 2003 Web Server	39

1. INTRODUCTION

The Web server is at the front-end of any organization's hosting infrastructure. It is directly connected to the Internet and is responsible for receiving requests from the clients of entire world, creating dynamic Web pages and responding with the requested data.

A secure web server provides a foundation for the organization's hosting environment, where its configuration plays a critical role in the overall security of the Web applications.

This guideline provides a step-by-step approach to secure the IIS 6.0 Web Server hosted on Windows 2003. All the recommended settings and instructions have been tested on IIS6.0 with MS Windows 2003 as operating system. It is assumed that the user has a basic knowledge of windows and IIS basic security concept.

The recommended settings mentioned in this guideline are indicative and may change according to the specific requirements in which the web server is running.

2. OVERVIEW OF IIS 6.0

IIS 6.0 is a complete web server available with all the versions of Microsoft Windows Server 2003. It is an enhancement of the previous version for reliability, manageability, security, scalability, and performance. Designed for intranets, the Internet, and extranets, IIS 6.0 makes it possible for organizations of all sizes to quickly and easily deploy powerful Web sites, applications, and Web services. In addition, IIS 6.0 provides a high-performance platform for applications built using the Microsoft .NET Framework and allows the distribution of files across the Internet or a network.

IIS 6.0 is not installed by default on all members of the Windows Server 2003 family, except for Windows 2003 Web Edition, it has to be explicitly selected and installed. IIS 6.0 will also be disabled when a server is being upgraded to Windows Server 2003, unless the IIS 5.0 Lockdown Tool has been installed prior to upgrade, or unless a registry key has been configured.

IIS 6.0 is configured in a locked-down state when installed. After installation, IIS 6.0 accepts requests for only static files until configured to serve dynamic content, and all time-outs and settings are set to aggressively secure defaults. Programmatic functionality provided by Internet Server API (ISAPI) extensions or Common Gateway Interfaces (CGI) must be manually enabled by an IIS 6.0 administrator.

2.1 Salient Architectural Features of IIS 6.0

The basic components of IIS 6.0 are explained below:

Application isolation is the separation of applications by process boundaries that prevents one application or Web site from affecting another and reduces the time that is being spend restarting services to correct problems related to applications.

Worker process is user-mode code whose role is to process requests, such as returning a static page or invoking an Internet Server API (ISAPI) extension or filter. Worker processes use HTTP.sys to receive requests and send responses over HTTP.

HTTP Protocol Stack (HTTP.sys): It is the HTTP listener and is implemented as a *kernel-mode*[1] device driver which is a part of networking subsystem of the Windows operating system. It protects the operating system kernel from the effects of imperfect application code, handles kernel-mode queuing and kernel-mode caching.

WWW Service Administration and Monitoring: This component is hosted in Svchost.exe, it runs in *user-mode*[2] and manages the lifetime of the worker process.

Inetinfo.exe: It is a user-mode component that hosts the IIS metabase and non-Web services of IIS 6.0, including the FTP service, the SMTP service, and the NNTP service. It depends on IIS Admin service to host the metabase.

[1] Kernel mode is the privileged processor mode in which operating system executive code runs. A driver or thread running in kernel mode has access to system memory and hardware.

[2] User-mode application cannot directly access hardware or use kernel-mode resources.

IIS Metabase: It is a plaintext, XML data store that contains most IIS configuration information (a few settings are maintained in the Windows registry). This new XML metabase allows administrators to directly read and edit the configuration file without using scripts or code, by using a common text editor such as Notepad. The XML metabase makes it easier to diagnose potential metabase corruption, and to back up and restore metabase files.

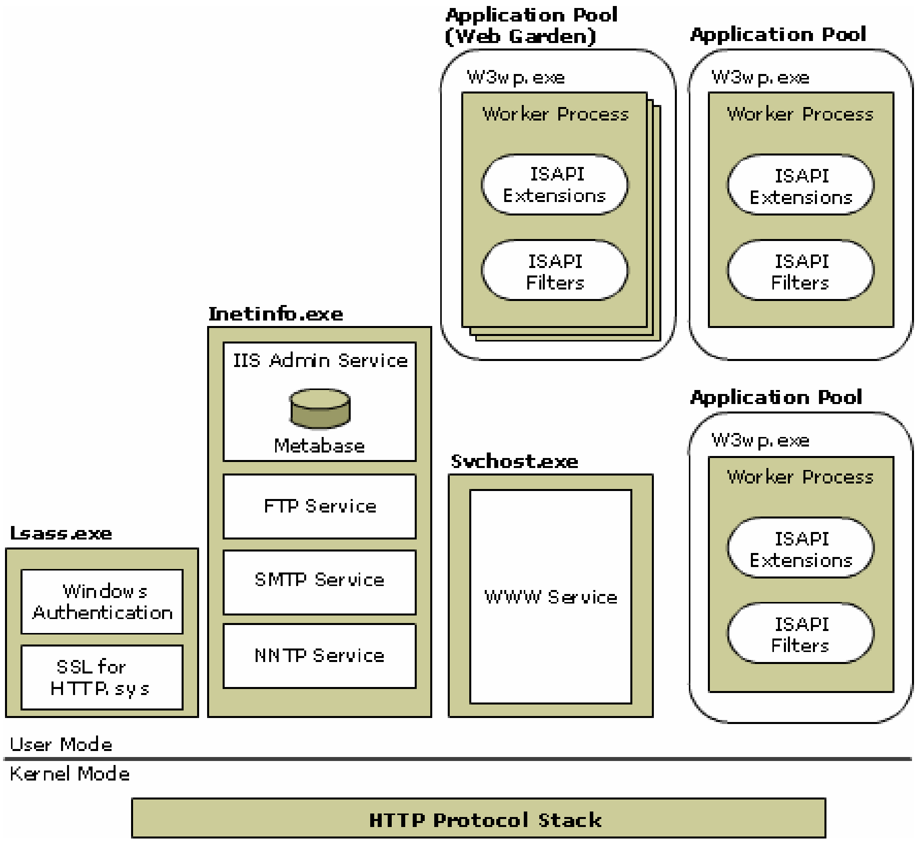

Figure-1: Architecture of IIS 6.0 (source: Microsoft Technet)

IIS 6.0 runs the server in one of two distinct request processing models, called application isolation modes. Application isolation is configured differently for each of the two IIS application isolation modes. Both modes rely on the *HTTP protocol stack* (also referred to as *HTTP.sys*) to receive Hypertext Transfer Protocol (HTTP) requests from the Internet and return responses. HTTP.sys resides in *kernel mode*, where operating system code, such as device drivers, runs and listens for & queues, HTTP requests.

The new request-processing architecture and application isolation environment enables individual Web applications, which always run in user mode, to function within a self-contained worker process with no dependence on a central process such as Inetinfo.exe to load and execute the application. All requests are handled by worker processes that are isolated from the Web server itself.

In this application isolation mode, Web applications can be grouped into *application pools*[3], through which configuration settings can be applied to the worker processes that service those applications. Process boundaries separate each application pool so that when an application is routed to one application pool, applications in other application pools do not affect that application. By using application pools, all application code can be run in an isolated environment without incurring a performance penalty.

[3] An application pool is a grouping of Web sites or applications served by the same worker process.

3. HOST SECURITY

Before the hardening of the IIS web server it is important that the under lying OS should be hardened and unwanted services should be stopped. It is the most essential part to reduce the attack vectors.

The following steps should be taken in this regard:

- Implement physical security for System.
- Harden the file system (preferably use NTFS).
- Remove NTFS permissions that are granted to the "Everyone" group on the root folder of all disk volumes.
- Only required services should be enabled. [Refer to Annexure-I for reference].
- Restrict anonymous registry access.
- Ensure that the system files and the registry are protected using strong access control list
- Hardening of TCP/IP Stack to avoid DoS attacks.
- Limit user accounts. Remove all user accounts which are not required.
- Strong Password Policy should be enforced.
- Do not use programs from un-trusted sources.
- Remove any compilers or development environments, from the web server.
- Remove un-necessary DSNs (Domain Source Names), as these contains clear text connection details used by applications to connect to OLE DB data sources. Only those DSNs required by Web applications should be installed.
- Ensure that security patches and service packs are up-to-date.
- Maintain updated antivirus software.
- Apply proper security templates in the local security policy.

Follow specific best practices guidelines for the operating system, issued by Microsoft and CERT-In.

4. SECURE IIS CONFIGURATION

4.1 Minimized Default Installation

4.1.1 Essential IIS Components and Services

In Addition to the WWW Service in IIS 6.0 includes other services such as FTP and SMTP service. To secure the web server it is essential to enable only those services which are required for the web site or the web application to run properly. The important IIS 6.0 services and components with their recommended settings are given below:

Table 1: Subcomponents of Internet Information Services (IIS)

Subcomponent	Default Setting	Recommended Setting	Comment
Background Intelligent Transfer Service (BITS) server extension	Disabled	See comment	BITS is a background file transfer mechanism used by applications such as Windows Updates and Automatic Updates. Enable this component if a software depends on it, such as Windows Updates or Automatic Updates to automatically apply service packs, hot fixes, or install other software on the Web server.
Common Files	Enabled	No change	On a dedicated Web server, these files are required by IIS and must always be enabled.
File Transfer Protocol (FTP) Service	Disabled	No change	Allows the Web server to provide FTP services. This component is not required on a dedicated Web server. However, it might be needed to enable FTP on a server that is only used for posting content, to support software such as Microsoft FrontPage® 2002 without enabling FrontPage 2002 Server Extensions. Because the FTP credentials are always sent in plaintext, it is recommended that user should connect to FTP servers through a secured connection, such as those provided by IPSec or a VPN tunnel.

Table 1: Subcomponents of Internet Information Services (IIS)

Subcomponent	Default Setting	Recommended Setting	Comment
FrontPage 2002 Server Extensions	Disabled	See comment	Provides FrontPage support for administering and publishing Web sites. On a dedicated Web server, disable when no Web sites are using FrontPage Server Extensions.
Internet Information Services Manager	Enabled	See comment	Administrative interface for IIS. Disable if user do not want to administer the Web server locally.
Internet Printing	Disabled	No change	Provides Web-based printer management and allows printers to be shared by using HTTP. This component is not required on a dedicated Web server.
NNTP Service	Disabled	No change	Distributes, queries, retrieves, and posts Usenet news articles on the Internet. This component is not required on a dedicated Web server.
SMTP Service	Enabled	Disabled	Supports the transfer of electronic mail. This component is not required on a dedicated Web server.
World Wide Web Service	(See Table 2 for subcomponents)	No change	Provides Internet services, such as static and dynamic content, to clients. This component is required on a dedicated Web server. Note: If this component is not enabled, then all subcomponents are not enabled.

Table 2: Subcomponents of the World Wide Web Service			
Subcomponent	**Default Setting**	**Recommended Setting**	**Comment**
Active Server Pages	Disabled	See comment	Provides support for Active Server Pages (ASP). Disable this component when none of the Web sites or applications on the Web server uses ASP.
Internet Data Connector	Disabled	See comment	Provides support for dynamic content provided through files with .idc extensions. Disable this component when none of the Web sites or applications on the Web server includes files with .idc extensions.
Remote Administration (HTML)	Disabled	No change	Provides an HTML interface for administering IIS. Use IIS Manager instead to provide easier administration and to reduce the attack surface of the Web server. This component is not required on a dedicated Web server.
Remote Desktop Web Connection	Disabled	No change	Includes Microsoft ActiveX® controls and sample pages for hosting Terminal Services client connections. Use IIS Manager instead to provide easier administration and to reduce the attack surface of the Web server. This component is not required on a dedicated Web server.
Server-Side Includes	Disabled	See comment	Provides support for .shtm, .shtml, and .stm files. Disable this component when none of the Web sites or applications on the Web server includes files with these extensions.
WebDav Publishing	Disabled	Disabled	Web Distributed Authoring and Versioning (WebDAV) extends the HTTP/1.1 protocol to allow clients to publish, lock, and manage resources on the Web. Disable this component on a dedicated Web server.
World Wide Web Service	Enabled	No change	Provides Internet services, such as static and dynamic content, to clients. This component is required on a dedicated Web server.

It is recommended that user should follow the 'Recommended Settings' mentioned in the above table, according to their requirement. The above mentioned subcomponents can be enabled or disabled in **Add or Remove Windows Components**, which is accessible from **Add or Remove Programs** in Control Panel, or in the Web Service Extensions node in IIS Manager.

4.1.2 Delete the Default Web Site

The IIS 6.0 gets installed in lockdown mode by default, however it still contains a default website and sample files. Several UDDI (Universal Description, Discovery, and Integration) aspx samples are configured on the default site and it is suggested to remove the default website and start with new.

4.1.3 Web Services Extensions

IIS 6.0 is configured in a locked-down state when installed. After installation, IIS 6.0 accepts requests for only static files until configured to serve dynamic content. To host the dynamic content such as ASP, ASP .NET required web services extensions should be enabled. These extensions are ASP .NET, WebDAV, SSI, and Front Page Extensions. Enable the web server extension only if it is required by the website or application. It is recommended that only necessary Web service extensions should be enabled.

To enable Web service extensions

1. In IIS Manager, click the **Web Service Extensions** folder.
2. In the details pane, select the Web service extension that you want to enable, and then click **Allow**.
3. To check the properties of a Web service extension, select an extension, and then click **Properties**.

Table3: Predefined Web Service Extensions

Web services Extensions	**Recommendations**
Active Server Pages	Enable if the website or application contains Active Server Pages (ASP) content
ASP.NET v1.1.4322	Enable if the website or application contains ASP .NET content
FrontPage Server Extensions 2002	Enable if the website or application uses FrontPage Extensions
Internet Data Connector (IDC)	This includes .idc and .idx files which are required to display the database information, if the website required Internet Data Connector then only it should be enabled.
Server Side Includes (SSI)	Server Side Includes are reusable contents such as Webpage Header, footer etc. These are directives to initiate IIS servers to insert reusable content on the webpage. Enable only if they are required.
Web Distributed Authoring and Versioning (WebDav)	WebDAV extension used for authorized users to remotely add and manage content on a Web server. This Web service extension is not recommended on a dedicated Web server.

For each Web service extension that is used by Web sites and applications and that is not one of the default Web service extensions, add a new entry to the Web service extensions list and configure the status of the new entry to ***Allowed.***

4.1.4 Disable FileSystemObject (FSO) Component

The FileSystemObject (FSO) component is used to create, delete, gain information about folders and files etc. This is used by the ASP, Application Script and other windows scripts. It is recommended to disable the **FileSystemObject** (FSO) if it is not required.

To disable the FileSystemObject component

1. Open the Command Prompt window
2. Set to the *%systemdrive%*\Windows\system32 directory
3. Type **regsvr32 scrrun.dll /u** and press **Enter** the following message will appear "DllUnregisterServer in scrrun.dll succeeded."
4. Click **OK.**
5. **Exit** to close the command prompt window

4.1.5 Enable Only Essential MIME Types

IIS 6.0 serves only the static files with extensions that are registered in the Multipurpose Internet Mail Extensions (MIME) types lst. IIS 6.0 is preconfigured to recognize a default set of global MIME types, which are recognized by all configured Web sites. MIME types can be defined at the Web site and directory levels, independently of one another or the types defined globally. IIS also allows changing, removing, or configuring additional MIME types. For any static content file extensions used by the Web sites and hosted on IIS, that are not defined in the MIME types list, the corresponding MIME type entry must be created.

Configure the MIME types by completing the following steps:

Configure MIME Types

To add a global MIME type

1. In **IIS Manager**-right-click the **local computer**-click **Properties**-click **MIME Types** button-click **New**-in the **Extension** box, type the file name extension.

2. In the **MIME type** box, type a description that exactly matches the file type defined on the computer- Click **OK**.

To add a MIME type to a Web site or directory:

1. In **IIS Manager**-right-click the Web site or Web site directory for which adding a MIME type- click **Properties**- Click **HTTP Headers** – Click **Mime Types**- Click **New**- In the **Extension** box, type the file name extension.
2. In the **MIME type** box, type a description that exactly matches the file type defined on the computer. If define a MIME type that has already been defined at a higher level, you are prompted to select the level where the MIME type should reside- Click **OK.**

4.2 User Rights and Permissions

4.2.1 IIS User Accounts

IIS server has a various built-in accounts in addition to the windows accounts. If an application or a worker process is runing with a high level privilege, such as LocalSystem user account this could be a security risk. A malicious user can gain access to the LocalSystem user privilege.

LocalSystem

LocalSystem has default user right of "Full access". This is the part of the Administrators group with high level access rights. If a worker process runs as the LocalSystem user account, then that worker process has full access to the entire system.

Network Service

The Network Service user account interacts with the other system having credentials of the computer account. The built-in Network Service user account has fewer access rights on the system than the LocalSystem user account. In IIS 6.0, it is suggested that the worker process identity that is defined for application pools runs as the Network Service user account. This account has following default user rights:

1. Replace a process-level token (SeAssignPrimaryTokenPrivilege)
2. Adjust memory quotas for a process (SeIncreaseQuotaPrivilege)
3. Generate security audits (SeAuditPrivilege)
4. Bypass traverse checking (SeChangeNotifyPrivilege)
5. Access this computer from a network (SeNetworkLogonRight)
6. Log on as a batch job (SeBatchLogonRight)
7. Log on as a service (SeInteractiveLogonRight)
8. Allow log on locally (SeInteractiveLogonRight)

Local Service

The Local Service user account has the same access right as the Network Service user account with limited user right to the local computer. If a worker process does not require access to the external server then it runs under the Local Service user. The Local Service has the following default user rights:

1. Replace a process-level token (SeAssignPrimaryTokenPrivilege)
2. Adjust memory quotas for a process (SeIncreaseQuotaPrivilege)
3. Generate security audits (SeAuditPriv ilege)
4. Bypass traverse checking (SeChangeNotifyPrivilege)
5. Access this computer from a network (SeNetworkLogonRight)
6. Log on as a batch job (SeBatchLogonRight)

IIS_WPG

The IIS IIS_WPG group account has the minimum permissions and user rights which are necessary to start up and run a worker process on a Web server. The IIS_WPG has the following default user rights:

1. Bypass traverse checking (SeChangeNotifyPrivilege)
2. Log on as a batch job (SeBatchLogonRight)
3. Access this computer from a network (SeNetworkLogonRight)

IUSR_*ComputerName*

If the website is mapped to the IUSR_*ComputerName* account it uses the anonymous authentication. This account is used for anonymous access to IIS. IUSR_*ComputerName* has the following default user rights:

1. Access this computer from a network (SeNetworkLogonRight)
2. Bypass traverse checking (SeChangeNotifyPrivilege)
3. Log on as a batch job (SeBatchLogonRight)
4. Allow log on locally (SeInteractiveLogonRight)

IWAM_*ComputerName*

The IIS IWAM_*ComputerName* user account is for starting out-of-process applications in isolation mode. IWAM_*ComputerName* has the following default user rights:

1. Replace a process-level token (SeAssignPrimaryTokenPrivilege)
2. Adjust memory quotas for a process (SeIncreaseQuotaPrivilege)
3. Bypass traverse checking (SeChangeNotifyPrivilege)
4. Access this computer from a network (SeNetworkLogonRight)
5. Log on as a batch job (SeBatchLogonRight)

ASPNET

The built-in ASPNET user account is for running the ASP.NET worker process in isolation mode. ASPNET has the following default user rights:

1. Access this computer from a network (SeNetworkLogonRight)
2. Log on as a batch job (SeBatchLogonRight)
3. Log on as a service(SeInteractiveLogonRight)
4. Deny logon locally (SeDenyInteractiveLogonRight)
5. Deny logon through Terminal Services (SeDenyRemoteInteractiveLogonRight)

4.2.2 Authentication

This is the identification process for the authorization. This can be set on the complete website or the specific file and directory of the website. Authentication helps to control the access of web directory or file by the unauthorized user. There are various ways to authenticate the user on the website

Anonymous authentication

This authentication method allows everyone to access the Web site, without asking for a user name or password.

Integrated Windows Authentication:

This authentication method uses hashing technology to identify users. The credentials are not sent over the network.

To enable Integrated Windows Authentication perform the following steps

1. In **ISS Manager**, double-click the **local computer**
2. Right-click the **Web Sites folder**, virtual directory, or a file; and then click **Properties**.
3. Click the **Directory Security** or **File Security** tab, and then, in the Authentication and access control section, click **Edit**
4. In the **Authenticated access** section, select the **Integrated Windows Authentication** check box.
5. Click **OK** twice.

Digest Authentication:

The Digest authentication method is used to authenticate user name and password information. This transmits the passwords across the network in a hash value. This type of authentication is available only on domains with domain controllers running Windows server operating systems.

To enable Digest authentication perform the following steps:

1. In **ISS Manager**, double-click the **local computer**
2. Right-click the **Web Sites folder**, virtual directory, or a file; and then click **Properties**.
3. Click the **Directory Security** or **File Security** tab, and then, in the Authentication and access control section, click **Edit**
4. In the **Authenticated access** section, select the **Digest authentication for Windows Server** check box.
5. Click **OK** twice.

Basic Authentication:

The Basic authentication method is generally used for collecting user name and password information. This method transmits user names and passwords across the network in an unencrypted form. This can be secured by the Web server's encryption features, with combination of Basic authentication. To enable Basic authentication perform the following steps:

1. In **ISS Manager**, double-click the **local computer**
2. Right-click the **Web Sites folder**, virtual directory, or a file; and then click **Properties**.
3. Click the **Directory Security** or **File Security** tab, and then, in the Authentication and access control section, click **Edit**
4. In the **Authenticated access** section, select the **Basic authentication** check box.

.NET Passport Authentication

This is user authentication service that provides Web site users to create a single sign-in and password for access to all .NET Password enabled Web sites and Applications. The user will authenticate by the .NET Passport central server. To use this process first ensure that the IIS server and the .NET Passport server are communicating properly. A comparison of Web Site authentication methods is given below:

Table 4: Comparison of Web Site Authentication Methods			
Method	**Security Level**	**How Passwords Are Sent**	**Crosses Proxy Servers and Firewalls**
Anonymous authentication	None	N/A	Yes
Basic authentication	Low	Base64 encoded clear text	Yes, but sending passwords across a proxy server or firewall in clear text is a security risk because Base64 encoded clear text is not encrypted.
Digest authentication	Medium	Hashed	Yes
Advanced Digest authentication	Medium	Hashed	Yes
Integrated Windows authentication	High	Hashed when NTLM is used; Kerberos ticket when Kerberos is used.	No, unless used over a PPTP connection
Certificate authentication	High	N/A	Yes, using an SSL connection
.NET Passport authentication	High	Encrypted	Yes, using an SSL connection

4.2.3 Metabase Permissions

The Metabase file contains all the configuration information of the IIS web server, earlier this was a binary file in IIS 4 & IIS 5. In IIS 6.0 it has been replaced with a single binary file having two XML files (MetaBase.xml and MBSchema.xml). Always keep the backup of the MetaBase file. Configuration of the Metabase file should always be restricted. Only the members of the Administrative group and local system account should have full control to this file. IIS stores these files in the *%systemroot%*\System32\Inetsrv folder of the computer.

The metabase consists of the following elements:

- **MetaBase.xml file:** This file stores IIS configuration information that is specific to an installation of IIS.
- **MBSchema.xml file:** This file contains the metabase schema. The MBSchema.xml file is a master configuration file that defines default attributes for all metabase properties and enforces rules for constructing and placing metabase entries within the metabase.
- **In-memory metabase.** The in-memory metabase contains the most current metabase and metabase schema configuration. The in-memory metabase accepts changes to the metabase configuration and schema, storing them in

RAM, and periodically writing changes to the on-disk metabase and metabase schema files.

To restrict access to the MetaBase.xml file

1. Click **Start**, right-click **My Computer**, and then click **Explore**.
2. Browse to the *%systemdrive%*\Windows\System32\Inetsrv\MetaBase.xml file, right-click the file, and then click **Properties**.
3. Click the **Security** tab, confirm that only members of the Administrators group and the LocalSystem account have Full Control access to the metabase, remove all other file permissions, and then click **OK.**

To restrict access to the MBschema.xml file

1. Click **Start**, right-click **My Computer**, and then click **Explore**.
2. Browse to the *%systemdrive%*\Windows\System32\Inetsrv\MBschema.xml file, right-click the file, and then click **Properties**.
3. Click the **Security** tab, confirm that only members of the Administrators group and the LocalSystem account have Full Control access to the metabase, remove all other file permissions, and then click **OK.**

4.2.4 Fine-Tune Metabase Settings

IIS uses various settings that aren't directly available from IIS Manager. These settings can help to stop or limit attacks. For example, buffer overflow attacks flood a Web site with large amounts of data. IIS 6.0 lets to use the MaxRequestEntityAllowed and AspMaxRequestEntityAllowed metabase settings to limit the entity body size of a request or an Active Server Pages (ASP) request, respectively. These settings allow setting the maximum size, in bytes, for the body of a request, as specified in the HTTP content-length header. Use the IIS Metabase Explorer tool to edit the metabase.

Metabase Explorer is included in the Microsoft IIS 6.0 Resource Kit Tools, which you can download from:

http://www.microsoft.com/downloads/details.aspx?familyid=56fc92ee-a71a-4c73-b628-ade629c89499&displaylang=en

Table 5 shows some metabase settings that should be considered changing.

Table 5: IIS Metabase Settings		
Setting	**Default Value**	**Comments**
AspKeepSessionIDSecure	0	Set this value to 1 to ensure that session IDs are sent as a secure cookie if they're assigned over a secure channel.
AspMaxRequestEntityAllowed	200000	Sets the maximum number of bytes allowed in the entity body of an ASP request. Reduce this value as appropriate for your site.
CGITimeout	300	Specifies the timeout, in seconds, for Common Gateway Interface (CGI) applications. Reduce this value as appropriate for your site.
MaxRequestEntityAllowed	4294967295	Specifies the maximum number of bytes allowed in the entity body of a request. Reduce this value as appropriate for your site.

4.2.5 Securing IIS Web Site Permissions

In IIS 6.0, Web site permissions can be set, which allows controlling access to a Web site or virtual directory. IIS examines Web site permissions to determine which type of action can occur, such as accessing the source code of a script or browsing folders.

Following table lists and describes the Web site permissions that are supported by IIS 6.0.

Table 6: Web Site Permissions That Are Supported by IIS 6.0	
Permission	**Description**
Read	Users can view the content and properties of directories or files. This permission is set by default. This permission is required for Web sites that have static content. If all of your content is scripted, such as a Web site that only uses ASP content, you can remove the Read permission.
Write	Users can change content and properties of directories or files.
Script Source Access	Users can access source files. If the Read permission is set, then users can read source files; if the Write permission is set, then users can modify the content and properties of the source files. The Script Source Access permission also applies to the source code for scripts. This option is not available if both the Read and Write permissions are not set. Set this permission only when using WebDAV. In addition, make sure that user requires authentication for this site and that the file permissions are set correctly. **Important**: When the Script Source Access permission is set, users might be able to view sensitive information, such as a user name and password. Users might also be able to change source code that runs on the server, and seriously affect the

Table 6: Web Site Permissions That Are Supported by IIS 6.0	
Permission	**Description**
	security and performance of the server.
Directory browsing	Users can view file lists and collections.
Log visits	A log entry is created for each visit to the Web site. As an operational security practice, it is highly recommended to enable logging.
Index this resource	Indexing Service can index this resource. This allows searches to be performed on the resource.
Execute	Users have the appropriate level of script execution: • **None.** Does not allow scripts or executables to run on the server. • **Scripts only.** Allows only scripts to run on the server. • **Scripts and Executables.** Allows both scripts and executables to run on the server.

Use appropriate Web site permissions as given above in conjunction with NTFS permissions to allow users to access desired content. Web site permissions can be set for specific sites, directories, and files. Unlike NTFS permissions, Web site permissions affect everyone who tries to access your Web site.

If Web site permissions conflict with NTFS permissions for a directory or file, the more restrictive settings are applied.

4.2.6 Securing the Web Site Directory and Content

To protect against the attack such as directory traversal attacks, the web root directory should always relocate to a non-system partition. The access rights helps to protect the file and the directory from the unauthorized access. Configure the NTFS permissions on the root of the disk volume so that:

- Only Administrators group has full control.
- All other permissions are removed.

To move Web site content to a nonsystem drive:

1. Open **Information Services (IIS) Manager.**
2. Right-click the Web site, and then click **Stop**
3. Open Command Prompt window
4. **xcopy** *%systemdrive%***inetpub\wwwroot\SiteName <Drive>:\wwwroot\SiteName /s /i /o**
5. Go back to the **Internet Information Services (IIS) Manager**
6. Right-click the Web site and then click **Properties**
7. Click the **Home Directory** and set the new path
8. Start the Web site.

Access control lists

Access control lists (ACLs) indicate which user/s or group/s have permission to access or modify a particular file. The following table provides some recommendations on the NTFS permissions that should be applied to the different file types on an IIS server. These file types can be grouped in separate folders to simplify the process of applying NTFS permissions.

Permissions for the content should be given as follows

Table 7: NTFS Permissions for different files

File Type	Recommended NTFS Permissions
CGI files (.exe, .dll, .cmd, .pl)	Everyone (execute) Administrators (full control) System (full control)
Script files (.asp)	Everyone (execute) Administrators (full control) System (full control)
Include files (.inc, .shtm, .shtml)	Everyone (execute) Administrators (full control) System (full control)
Static content (.txt, .gif, .jpg, .htm, .html)	Everyone (read – only) Administrators (full control) System (full control)

4.2.7 Setting IP Address and Domain Name Restrictions

One method of protecting the Web sites and applications that are hosted on the server is to restrict access from specific IP addresses or domain names. Any combination of IP address ranges or domain names can explicitly grant or deny access.

By restricting access to Web sites and applications by using IP address ranges or domain names, grant or deny access permissions to a specific set of computers or to an organization can be given. The restrictions that are specified affect the entire Web site or application and cannot be configured for individual portions of the Web site or application.

Restrict access to a specific Web site for a specific IP address range or domain name by completing the following steps:

1. Specify the default access that will be given to the majority of users accessing the application by doing one of the following:

    - To allow the majority of users to access the application, enable default access.
    - To allow a limited number of users to access the application, disable default access.

2. For each computer, or group of computers, that administrator wants to grant or deny access, specify the IP address range or domain name for the clients that are exceptions to the default access specified in Step 1.

   If the administrator is unable to identify the IP address range for the computers, he should specify the domain name. From a performance perspective, specifying the IP address range is preferred. If a domain name is specified, DNS reverse lookups must be done each time a user accesses the application and the performance of the application is degraded.

   Specify the IP address range in the form of a single IP address or a network ID with a corresponding subnet mask.

4.2.8 Isolating Applications

When a Web server hosts multiple Web sites and applications, each Web site and application requires a certain level of isolation, to prevent from adversely interacting with one another.

When IIS 6.0 is running in worker process isolation mode, Web sites and applications hosted on the same Web server can be isolated by specifying that the Web sites and applications belong to separate *application pools.* Application pools can be used to prevent the Web sites and applications running in one application pool from accessing the content contained in another application pool which improves the security and reliability of the web server. To enhance the availability of Websites and applications, isolate unstable web sites and applications in a separate application pools.

For each application pool, an application pool identity can be specified, which is a user account that is assigned to an application pool. After specifying the application pool identity, assign permissions (such as NTFS permissions or SQL database permissions) for each application pool identity. Because individual application pools can use different identities, selectively grant or deny resource access to an application pool. The Web sites and applications running in an application pool have the same user rights and resource permissions assigned to the application pool identity.

Run the process with the minimum permissions required for the application. The application could be configured into following three levels:

1. Process – Low level application protection.
2. Pooled – Medium level application protection.
3. Isolated – High level application protection.

To create an application pool

1. Open **Internet Information Services (IIS) Manager.**
2. Double-click the **local computer**, right-click **Application Pools**, click **New**, and then click **Application Pool**.

3. In the **Application pool ID** box, type a **new ID** for the application pool
4. Under **Application pool settings**, click **Use default settings for the new application pool**, and then click **OK.**

To assign a Web site or application to an application pool

1. Open **Internet Information Services (IIS) Manager.**
2. Right-click the Web site or application and click **Properties**.
3. Click the **Home Directory** tab.
4. In the **Application pool** list box, select the name of the application pool to and then click **OK.**

4.2.9 Evaluating the Effects of Impersonation on Application Compatibility

Securing Web sites and applications by isolating them into separate application pools with unique identities can cause application compatibility problems when other than anonymous access is used. The application compatibility problems arise from the complexities of impersonation[4].

When a worker process is created by the WWW service, it is created with a process token that is associated with the application pool identity. This establishes the process identity of the worker process. By default, all of the actions taken by the worker process are completed in the context of this worker process identity account. However, when a client request is processed, the thread that processes the request uses a token associated with the client, which is also known as the *authenticated user's token,* during the duration of the request.

Before IIS serves a URL, the authenticated user's token is verified against the access control list (ACL) of the resource that is being requested. Additionally, if the request is for an ISAPI extension, such as ASP, the worker process applies the authenticated user's token as an impersonation token to the thread that calls the ISAPI extension. When the ISAPI extension begins processing the request, this impersonation token applies to the actions it takes. Consequently, the actions taken by an ISAPI extension are associated with the authenticated user, not the process identity.

Thus it is recommended to evaluate the effects of impersonation behavior on compatibility for the ASP applications & ASP.NET applications

4.2.10 Configure Web Sites and Applications for Isolation

Running worker processes under different identities can cause application compatibility problems, especially for Web sites that use user authentication. Complete the following steps to identify when Web sites and applications require isolation for security reasons:

[4] Impersonation allows a worker process to run under security credentials that are different from its base identity.

1. Create a list of the Web sites and applications to be hosted on the Web server.
2. Group the Web sites and applications by organization (or business unit within an organization if all of the Web sites and applications hosted on the Web server are owned by one organization).
3. Subdivide each group created in the previous step into smaller groups of Web sites and applications that require the same user rights and resource access.
4. For each group created in the previous step, create a new application pool to be used by the Web sites and applications within the pool.
5. Assign the Web sites and applications within each group to the corresponding application pool.
6. For each application pool, create a service account, to be used as the application pool identity.

   In IIS, the default identity for newly created application pools is NetworkService. To ensure proper assignment of permissions to resources, create a new *service account*[5].

   In addition, add the service account to the IIS_WPG group to provide the appropriate access to the IIS metabase and content. The IIS_WPG group is granted the appropriate user rights and resource permissions to allow most Web sites and applications to run properly.

7. Assign any additional user rights[6] to the application pool identities.

   The user rights granted to the IIS_WPG group are sufficient for most Web sites applications. When the user rights granted to the IIS_WPG group are insufficient, grant only the user rights to the user account, which is used as the identify for the application pool, that are necessary to ensure the appropriate operation and behavior of the application. Ensure that any non-essential user rights are removed to prevent the Web sites and applications from having elevated user rights.

8. Assign the service account identity to the corresponding application pool.
9. Assign the appropriate resource permissions, such as NTFS or SQL database permissions, to the application pool identities.

   Assign only the NTFS file and folder permissions that are necessary to ensure the appropriate operation and behavior of the application. By default, grant only read permissions to the application pool identity to ensure that the Web sites and applications in the application pool cannot modify the Web site content or other files on the Web server. If the applications require write access to any files and folders, consult the application developers to

[5] A service account is a user account that is created explicitly for the purpose of providing a security context for services running on Windows Server 2003.

[6] User rights authorize users to perform specific actions, such as logging on to a system interactively or backing up files and directories. User rights are different from permissions because user rights apply to user accounts, whereas permissions are attached to objects.

determine if the application can be modified so that write access is not required.

4.3 Other Security Configurations

4.3.1 Configure the custom error Pages

The attacker could gain some important information form error pages. The information about the server name, file path, Database name etc. should not be disclosed while error handling. The server gives default error pages for the standard error code when it encounters an error. It is suggested to rewrite these pages and customized for the website. So as a malicious user could not get server details like installation path or application's details etc.

4.3.2 Configuring Secure Sockets Layer

The Secure Sockets Layer (SSL) protocol communicates between the Web server and Browser in encrypted and authenticated manner. It verifies the integrity of the content and the authenticity of the user SSL can be configured to provide security for any portion of the Web sites or applications on the Web server.

To configure Secure Sockets Layer perform the following steps

1. In **IIS Manager**, double-click the local computer, and then double-click the **Web Sites folder**.
2. Right-click the Web site or file that you want to protect with SSL, and then click **Properties**.
3. Under **Web site identification** click **Advanced**
4. In the **Advanced Web site identification** box, under **Multiple identities for this Web site**, verify that the Web site IP address is assigned to port 443, the default port for secure communications, and then click **OK**. Optionally, to configure more SSL ports for this Web site, click **Add** under **Multiple identities of this Web site**, and then click OK.
5. On the **Directory Security** or **File Security** tab, under **Secure communications**, click **Edit**.
6. In the **Secure Communications** box, select the **Require secure channel (SSL)** check box
7. To enable SSL client certificate authentication and mapping features, select the **Enable client certificate mapping** check box, click **Edit**, add the 1-to-1 or many-to-1 mappings as you need, and then click **OK** three times.

4.3.3 Logging

Logging is a vital part of the security of the IIS 6.0 Server, which is helpful to determine any suspicious or unauthorized activity on the server. Log file should be regularly analyzed and archived securely. An alert mechanism should be placed to identify if any suspicious activity is going on.

Depending on the amount of traffic to the Web site, the size of the log file (or the number of log files) can consume valuable disk space, memory resources, and CPU cycles. Administrator might need to balance the gathering of detailed data with the need to limit files to a manageable size and number. If an administrator is planning to put thousands of Web sites on one Web server with high traffic volumes and disk writes, he might want to use centralized binary logging to preserve server resources. Also, consider limiting log size by changing the frequency of log file creation. The IIS logs allows to record events for each application and Web site on the Web server. Separate logs for each of the applications and Web sites can be created.

In IIS 6.0 the logging is done by the HTTP protocol stack (HTTP.sys). Server passes user-mode events to *HTTP.sys* through application programming interfaces (APIs), and then the user-mode events are logged by *HTTP.sys*. There are different log formats for IIS logs which support the following log formats.

W3C Extended log file format

World Wide Web Consortium (W3C) extended format is a customizable text format having different properties. Set log properties that are important as per the requirement, while limiting log size by omitting unwanted property fields. Properties are separated by spaces. To enable logging perform the following steps:

1. In **ISS Manager**, double-click the **local computer**
2. Right-click the **Web Sites folder**, virtual directory, or a file; and then click **Properties**.
3. Click the **Enable logging** check box.
4. In the **Active log format** list box, click a format. By default, the format is **W3C Extended Log File** Format
5. On the **Advanced** tab, select the properties you want to log.
6. Click **OK**

The log file can be customized by the selecting the necessary fields which are important to log. This can reduce the size of the log file. The various fields are given below:

Table 8: Log file fields

Property	Description
Client IP Address	The IP address of any client that accessed your server.
User Name	The name of the user who accessed your server.
Service Name	The Internet service running on the client computer.
Server Name	The name of the server on which the log entry was generated.
Server IP	The IP address of the server on which the log entry was generated.
Server Port	The port number the client is connected to.
Method	The action the client was trying to perform (for example, a GET command).
URI Stem	The resource accessed, such as an HTML page, a CGI program, or a script.
URI Query	The query, if any, the client was trying to perform. One or more search strings that the client was seeking to match are recorded in the log.
Protocol Status	The status of the action, in HTTP terms.
Win32 Status	The status of the action, in terms used by Windows.
Bytes Sent	The number of bytes sent by the server.
Bytes Received	The number of bytes received by the server.
Time Taken	The length of time the action took.
Protocol Version	The protocol (HTTP, FTP) version used by the client. For HTTP, this is either HTTP 1.0 or HTTP 1.1.
Host	The computer name.
User Agent	The browser used on the client.
Cookie	The content of the cookie sent or received, if any.
Referrer	The site that directed the user to the current site.
Protocol substatus	Additional status of the action, in HTTP terms.

IIS log file format

IIS log file format is fixed and cannot be customized. IIS format includes basic information, such as the user's IP address, user name, request date and time, service status code, and number of bytes received. In addition, IIS format also includes detailed items, such as the elapsed time, number of bytes sent, action (for example, a download carried out by a GET command), and target file. The items are separated by commas, making the format easier to read than the other ASCII formats, which use spaces for separators. The time is recorded as local time.

NCSA Common Log File Format

National Center for Supercomputing Applications (NCSA) Common format is a fixed ASCII format. This keeps basic information about user requests, such as remote host name, user name, date, time, request type, HTTP status code, and the number of bytes sent by the server. Items are separated by spaces; time is recorded as local time.

ODBC Logging

ODBC logging format is a record of a fixed set of data properties in a database that complies with Open Database Connectivity (ODBC). Some of the information logged includes the user's IP address, user name, request date and time (recorded as local time), HTTP status code, bytes received, bytes sent and action carried out.

When ODBC logging is enabled, IIS disables the kernel-mode cache which may degrade overall server performance.

Centralized Binary Logging

Centralized binary logging is the process by which multiple Web sites write binary, unformatted log data to a single log file. All Web sites log their activities into a single log file. It brings down load on CPU and memory resources and increase the performance and scalability of the server.

Secure Log File / Directory Locations

To set options for saving log files

1. In **ISS Manager**, double-click the **local computer**
2. Right-click the **Web Sites folder**, virtual directory, or a file; and then click **Properties**.
3. Select the log schedule to use when starting a new log file. The options are as follows:

    - **Hourly**: Log files created hourly, starting with the first entry that occurs for each hour. This option is typically used for high-volume Web sites.
    - **Daily**: Log files created daily, starting with the first entry that occurs after midnight.
    - **Weekly:** Log files created weekly, starting with the first entry that occurs after midnight on Saturday.
    - **Monthly:** Log files created monthly, starting with the first entry that occurs after midnight of the last day of the month.
    - **Unlimited file size:** Data is always appended to the same log file. You should access this log file only after stopping the site.
    - **When file size reaches:** A new log file is created when the current log file reaches a given size. Specify the size you want in the box.

4. Under **Log file** directory, type the directory where log files should be saved. [Either provide the full UNC path or map the path to a drive letter locally.]
5. Click **Apply,** and then click **OK** twice.

For details on centralized logging, refer to CERT-In guidelines "**Implementing Central Logging Server using syslog-ng**"

ACLs for the Log file

If the default log file directory is *%systemdrive%*\LogFiles. The *HTTP.sys* generates the following subdirectories, and the log files are created under these subdirectories:

1. For the W3C Extended, NCSA Common, and IIS log file formats, *HTTP.sys* generates the subdirectory *%systemdrive%*\LogFiles\W3SVC#, where # is the site ID.
2. For centralized binary logging, *HTTP.sys* generates the subdirectory *%systemdrive%*\LogFiles\W3SVC.
3. For *HTTP.sys* error logging, *HTTP.sys* generates the subdirectory *%systemdrive%*\WINDOWS\System32\LogFiles\HTTPErr.

By default, the log file directory has the following access control lists (ACLs):

1. NT Authority\System: **Full access**
2. Built-in\Administrators: **Full access**
3. Everyone: **No access**

Individual log files in the log file directory have the following controls:

1. NT Authority\System: **Full access**
2. Built-in\Administrators: **Read and delete access**
3. Everyone: **No access**

Apart from IIS logging, it is always recommended that the host security logging and web site content auditing should also be enabled.

The system and security logs are repositories for all events recorded on the Web server. System logs events can be configured by auditing[7]. The most common security events recorded by the Web server are associated with user accounts and resource permissions. With respect to web server, at a minimum, enable auditing on the following categories of events:

- Any changes to user account and resource permissions
- Any failed attempts for user logon
- Any failed attempts for resource access
- Any modification to the system files

[7] Auditing is the process that tracks the activities of users and processes by recording selected types of events in the security log of the Web server.

With respect to web site content, at a minimum, enable auditing for all users for any successful or failed attempts to do the following:

- Modify or delete existing content
- Create new content

4.3.4 Backup

The Backup helps to protect data from accidental loss due to system's hardware or storage media failure.

1. A proper Backup policy should be ensured.
2. The sensitive information which resides on the server such as Log file, Metabase file, Web site data etc should be protected in the same manner as server.
3. To prevent unauthorized access, restores should be controlled, with access provided only to administrator.
4. Protect individual backup or backup media by using passwords to protect against unauthorized restores. Backup data files should be on a secure partition with directory permissions set to prevent unauthorized users from gaining access to the files.
5. Take a routine backup of the web site or data on backup media.
6. To maintain the integrity of the file use the MD5 hash.

4.3.6 Network Security

TCP/IP port filtering

To minimize the TCP/IP-based security attacks on Web server it is suggested that only those ports should be opened which are required by the server. Ports which are not required should be blocked on the server as well as on the firewall. Always ensure that the associated ports which are required to run application effectively are enabled, because malicious users may attempt to exploit enabled ports to attack the server. This reduces the possibility of attack to the server and enhances the security of hosts also.

The details of the generally used TCP/ UDP Ports and Associated Services are as follows. User may decide to open the required ports as the need of application or website.

Table 9: TCP and UDP ports associated services

Default TCP Port Number	**Internet Service**
20	FTP Data Channel
21	FTP Control Channel
23	Telnet (enabled on some intranet or Internet servers)
25	Simple Mail Transfer Protocol (SMTP)
80	HTTP for World Wide Web
119	Network News Transfer Protocol (NNTP)
443	Hypertext Transfer Protocol over TLS/SSL (HTTPS) for secure

Table 9: TCP and UDP ports associated services

Default TCP Port Number	**Internet Service**
	World Wide Web
563	Network News Transfer Protocol over TLS/SSL (NNTPS)
Default UDP Port Number	**Internet Service**
53	DNS name queries (supports some Internet services)
161	SNMP

(Source: Microsoft)

4.3.6 Reviewing Security Policies, Processes, and Procedures

As a part of maintaining the security of Web server, the security policies, processes, and procedures in use by the organization should be reviewed periodically. Review the security practices for any changes that might affect the security of the Web server. These changes in security practices can include the following:

Ensuring that any recent security risks are mitigated:

Only good security practices helps to mitigate the security risks identified such as new viruses or new vulnerabilities. If current security practices do not address the new risks, then modify them to help in mitigating the risks.

Identifying changes in Web server configuration that can compromise security:

Through the course of normal administration of the Web server, configuration changes are made. During this process, security settings might have been inadvertently changed. Administrator need to periodically review the configuration of the Web server to ensure that it complies with the security requirements of the organization.

These security practices can be categorized by their function, such as operating system security, security policies, firewall security, and router security. In addition, the frequency with which these processes and procedures are completed varies. Some security practices need to be completed continuously while others might be completed monthly.

Following tables list examples of security policies, processes, and procedures grouped by categories. These examples are representative of the types of security practices that are required to maintain the security of the Web server.

Table 10: Windows Server 2003 Operating System Security

Security Policy, Process, or Procedure	Frequency
Limit user rights to only those that are required.	Constant
Limit any windows for vulnerabilities that can be exploited when deploying new servers.	Constant
Limit Terminal Services access to only necessary accounts.	Constant
Run a two-tier DNS structure to protect the identity of internal servers.	Constant
Run an Intrusion Detection System/ Intrusion Prevention System	Constant
Scan the ports in use on your server addresses and addresses assigned to remote users.	Daily
Review event and IIS logs.	Weekly
Test firewalls from inside and outside by using port scanners and other appropriate tools.	Weekly

Table 11: Windows Server 2003 Policy Security

Security Policy, Process, or Procedure	Frequency
Explicitly deny interactive logon user right to all non-administrative accounts.	Constant
Explicitly deny "Allow logon through Terminal Services" user right to all non-administrative accounts.	Constant
Enable FULL (Success/Failure) auditing on domain Group Policy objects.	Constant
Send event notification when events like "User added to Domain Administrators" occur.	Constant
Allow only Administrators to have write permissions on all content servers.	Constant
Require strong passwords for all users.	Constant
Require smart cards for all administrators.	Constant
Allow administrators to log on only to specific workstations.	Constant
Enable account lockout policies for failed logon attempts.	Constant
Audit the domain Group Policy object.	Monthly
Audit Active Directory user rights.	Monthly
Audit all servers to determine if nonessential services are running.	Monthly

Table 12: Firewall and Router Security

Security Policy, Process, or Procedure	Frequency
Restrict the network segments where management traffic is allowed.	Constant
By default, deny IP traffic and log any failed attempts.	Constant
Ensure that the minimal firewall rules are enforced, including:	Constant

Table 12: Firewall and Router Security

Security Policy, Process, or Procedure	**Frequency**
• Explicitly deny all traffic to the following: o TCP and UDP ports 135-139, 455 (NetBIOS/SMB) o TCP and UDP ports 3389 (Terminal Services) o Domain controllers o Internal DNS servers • Permit traffic to TCP and UDP port 53 (DNS) to external DNS servers.	

Table 13: Miscellaneous Security

Security Policy, Process, or Procedure	**Frequency**
Run virus scans on all servers.	Constant
Monitor security distribution lists and newsgroups for potential security issues.	Constant
During virus outbreaks, block any suspicious content (such as e-mail attachments).	Constant
Monitor the number of Non-Delivery mail reports generated (indicates e-mail spamming).	Weekly
Monitor SMTP relay attempts that are not valid (indicates e-mail spamming).	Weekly
Audit accounts to determine the users who are no longer employed at the organization, partner organizations, or customer organizations.	Monthly

5. CONTENT MANAGEMENT

5.1 Front page Server Extensions

Front page is used to maintain or upload the web site content. Before configuring the Front page Server Extensions ensure that they are made more secure and robust. After deploying the Front page Extension the following actions are suggested

- Prevent Local Account Creation
- Always Log Authoring Activities or details
- Prevent Executables from Being Uploaded
- Prevent Anonymous Write Permission
- Upgrade Server Extensions

5.2 Security considerations for content management

- Do all updates from the Intranet. Maintain the web page originals on a server on the Intranet and make all changes and updates here; then "push" these updates to the public server through an SSH or SSL connection.
- Write a script to download HTML pages and check against a template, note the changes occurred, if changes are as per the requirements, upload the correct version.

6. SECURE CODING

Sever administrators should ensure that the application or website code that the IIS server hosts, is as secure as possible. There are various flaws in the scripting which is used in the web application, these flaws in application allures the attacker. Some common security issues which should be considered before hosting a web application are as follows:

1. Audit the code before hosting on the Server.
2. Never rely on the client side data validation, use server side validation only.
3. Check the Proper input form validation to avoid the vulnerabilities/attacks such as SQL Injection[8], Buffer Over flow etc.
4. Run the web application with the least privilege as necessary to application.
5. To avoid the information leakages configure the application carefully so it can not disclose information regarding Server, Application or the Database.
6. Always use trusted component in the web application. Never use web components from untrusted sources.
7. Do not left comment code or any other credentials on the web page. This may help an attacker to gain information about the application or server and may lead to an attack.
8. Use strong password policy or encryption for user authorization. Never use common words for user authentication which is easy to guess.
9. Web site having discussion forum or other applications, where user post the data, always filter/sanitize the user input data to avoid the Cross Side Scripting (XSS) attack.
10. Cookies are used to maintain the session, it is suggested not to store the critical information such as credit card no, password, etc in plain text format on the client side cookies. Use one session token to reference properties and store the token in server-side cache.
11. Always check or analyze error log to track the authorized activities.

[8] For details on SQL injections, refer to CERT-In whitepaper “SQL Injection Techniques & Countermeasures”

7. SECURITY TOOLS

Various security tools are available to audit or to ensure the security of the Web server. It is recommended that auditing or penetration testing of Web server should be done periodically to mitigate the vulnerabilities. A list of some of free security tools available is as follows:

IIS Diagnostic Tools

http://www.microsoft.com/windowsserver2003/iis/diagnostictools/default.mspx

UrlScan Security Tool

http://www.microsoft.com/technet/security/tools/urlscan.mspx

IIS Lockdown Tool

http://www.microsoft.com/technet/security/tools/locktool.mspx

MS Web Application Stress Tool

http://www.microsoft.com/technet/archive/itsolutions/intranet/downloads/webstres.mspx?mfr=true

http://www.microsoft.com/downloads/details.aspx?FamilyID=E2C0585A-062A-439E-A67D-75A89AA36495&displaylang=en

Refer to CERT-In web site at the following link for the details of other security tools as per your requirements.

http://cert-in.org.in/securitytools.htm

8. REFERENCES

http://www.microsoft.com/resources/documentation/IIS/6/all/techref/en-us/iisRG_IIS_7.mspx#ECAA

http://www.microsoft.com/technet/security/guidance/secmod119.mspx#EIAA

http://cert-in.org.in/knowledgebase/guidelines/cisg-2003-09.pdf

http://www.microsoft.com/resources/documentation/iis/6/all/proddocs/en-us/gs_installingiis.mspx

Managing a Secure IIS 6.0 Solution:
http://www.microsoft.com/resources/documentation/IIS/6/all/techref/ en-us/iisRG_SEC.mspx

.NET Password authentication:
http://www.microsoft.com/resources/documentation/iis/6/all/proddocs/en-us/sec_auth_passport.mspx

Customizing W3C Extended Logging
http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/log_customw3c.asp

http://technet2.microsoft.com/windowsserver/en/technologies/featured/iis/default.mspx
http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/843df643-1dbb-4fb6-910d-ec1965fa9e43.mspx?mfr=true

Microsoft Windows Server 2003 Deployment Kit: Deploying Microsoft Internet Information Services (IIS) 6.0 by Microsoft Corporation

http://www.microsoft.com/resources/documentation/IIS/6/all/techref/en-us/iisRG_SEC_48.mspx

ANNEXURE-I

Table-14: Recommended Service Startup Types on a Dedicated Windows 2003 Web Server

Service Name	**Default Startup Type**	**Recommended Startup Type**	**Comment**
Alerter	Disabled	No change	Notifies selected users and computers of administrative alerts.
Application Layer Gateway Service	Manual	No change	Provides support for application-level plug-ins and enables network and protocol connectivity.
Application Management	Manual	See comment	Provides software installation services for applications that are deployed in **Add or Remove Programs** in Control Panel. On a dedicated Web server, this service can be disabled to prevent unauthorized installation of software.
Automatic Updates	Automatic	See comment	Provides the download and installation of critical Windows updates, such as security patches and hotfixes. This service can be disabled when automatic updates are not performed on the Web server.
Background Intelligent Transfer Service	Manual	See comment	Provides a background file-transfer mechanism and queue management, and it is used by Automatic Update to automatically download programs (such as security patches). This service can be disabled when automatic updates are not performed on the Web server.
ClipBook	Disabled	See comment	Enables the Clipbook Viewer to create and share data that can be reviewed by remote users.
COM+ Event System	Manual	No change	Provides automatic distribution of events to COM+ components.
COM+ System Application	Manual	No change	Manages the configuration and tracking of COM+-based components.
Computer Browser	Automatic	No change	Maintains the list of computers on the network, and supplies the list to programs that request the list.
Cryptographic Services	Automatic	No change	Provides three management services: Catalog Database Service, which confirms the signatures of Windows files; Protected Root Service, which adds and removes Trusted Root Certification Authority certificates from

Table-14: Recommended Service Startup Types on a Dedicated Windows 2003 Web Server			
Service Name	**Default Startup Type**	**Recommended Startup Type**	**Comment**
			the Web server; and Key Service, which helps in enrolling certificates.
DHCP Client	Automatic	No change	Required to automatically obtain IP configuration and to dynamically update records in DNS.
Distributed File System	Automatic	Disable	Manages logical volumes that are distributed across a local area network (LAN) or wide area network (WAN). On a dedicated Web server, disable Distributed File System.
Distributed Link Tracking Client	Automatic	Disabled	Maintains links between NTFS V5 file system files within the Web server and other servers in the domain. On a dedicated Web server, disable Distributed LinkTracking.
Distributed Link Tracking Server	Manual	Disabled	Tracks information about files that are moved between NTFS V5 volumes throughout a domain. On a dedicated Web server, disable Distributed Link Tracking.
Distributed Transaction Coordinator	Automatic	No Change	Coordinates transactions that span multiple resource managers, such as databases, message queues, and file systems.
DNS Client	Automatic	No change	Allows resolution of DNS names.
Error Reporting Service	Automatic	See comment	Collects, stores, and reports unexpected application crashes to Microsoft. If this service is stopped, then Error Reporting will occur only for kernel faults. On a dedicated Web server, disable Error Reporting Service.
Event Log	Automatic	No change	Writes event log messages that are issued by Windows-based programs and components to the log files.
Fax Service	Manual	Disabled	Provides the ability to send and receive faxes through fax resources that are available on

Table-14: Recommended Service Startup Types on a Dedicated Windows 2003 Web Server			
Service Name	**Default Startup Type**	**Recommended Startup Type**	**Comment**
			the Web server and network. On a dedicated Web server, this service can be disabled because sending and receiving faxes is not a typical function of a Web Server.
File Replication Service	Manual	No change	Enables files to be automatically copied and maintained simultaneously on multiple servers.
Help and Support	Automatic	No change	Enables Help and Support Center to run on the Web server.
HTTP SSL	Manual	No change	Implements the Secure Hypertext Transfer Protocol (HTTPS) for the HTTP service by using SSL. HTTP.sys automatically starts this service when any Web sites require SSL.
Human Interface Device Access	Disabled	No change	Enables generic input to Human Interface Devices (HIDs), which activates and maintains the use of predefined hot buttons on keyboards, remote controls, and other multimedia devices.
IMAPI CD-Burning COM Service	Disabled	No change	Manages CD recording by using the Image Mastering API (IMAPI).
Indexing Service	Manual	See comment	Indexes content and properties of files on the Web server to provide rapid access to the file through a flexible query language. On a dedicated Web server, disable this service unless Web sites or applications specifically leverage the Indexing Service for searching site content.
Internet Connection Firewall (ICF)/Internet Connection Sharing (ICS)	Disabled	No change	Provides network address translation (NAT), addressing and name resolution, and intrusion detection when connected through a dial-up or broadband connection. On a dedicated Web server, disable to prevent inadvertent enabling of NAT, which would prevent the Web server from communicating with the remainder of the network.
Intersite Messaging	Disabled	No changes	Required by Distributed File System (DFS).
IPSec Services	Automatic	No change	Provides management and coordination of

Table-14: Recommended Service Startup Types on a Dedicated Windows 2003 Web Server			
Service Name	**Default Startup Type**	**Recommended Startup Type**	**Comment**
			Internet Protocol security (IPSec) policies with the IPSec driver.
Kerberos Key Distribution enter	Disabled	No change	Provides the ability for users to log on using the Kerberos V5 authentication protocol.
License Logging Service	Disabled	No change	Monitors and records client access licensing for portions of the operating system, such as IIS, Terminal Services, and file and print sharing, and for products that are not a part of the operating system, such as Microsoft SQL Server or Microsoft Exchange Server. On a dedicated Web server, this service can be disabled.
Logical Disk Manager	Automatic	No change	Required to ensure that dynamic disk information is up to date.
Logical Disk Manager Administrative Service	Manual	No change	Required to perform disk administration.
Messenger	Disabled	No change	Transmits net sends and Alerter service messages between clients and servers.
Microsoft Software Shadow Copy	Manual	No change	Manages software-based volume shadow copies taken by the Volume Shadow Copy service. On a dedicated Web server, this service can be disabled when volume shadow copies are not used.
Net Logon	Manual	No change	Maintains a secure channel between the domain controller, other domain controllers, member servers, and workstations in the same domain and trusted domains.
NetMeeting Remote Desktop Sharing	Manual	Disabled	Eliminates potential security threats by allowing domain-controller remote administration through NetMeeting.
Network Connections	Manual	No change	Manages objects in the Network Connections directory.
Network DDE	Disabled	No change	Provides network transport and security for Dynamic Data Exchange (DDE) for

Table-14: Recommended Service Startup Types on a Dedicated Windows 2003 Web Server			
Service Name	**Default Startup Type**	**Recommended Startup Type**	**Comment**
			programs running on the Web server. This service can be disabled when no DDE applications are running locally on the Web server.
Network DDE DSDM	Disabled	No change	Used by Network DDE. This service can be disabled when Network DDE is disabled.
Network Location Awareness (NLA)	Manual	No change	Collects and stores network configuration and location information, and notifies applications when this information changes.
NTLM Security Support Provider	Manual	No change	Provides security to RPC programs that use transports other than named pipes, and enables users to log on using the NTLM authentication protocol.
Performance Logs and Alerts	Manual	See comment	Collects performance data for the domain controller, writes the data to a log, or generates alerts. This service can be set to automatic when you want to log performance data or generate alerts without an administrator being logged on.
Plug and Play	Automatic	No change	Required to automatically recognize and adapt to changes in the Web server hardware with little or no user input.
Portable Media Serial Number Service	Manual	No change	Retrieves the serial number of any portable media player that is connected to the computer.
Print Spooler	Automatic	See comment	Manages all local and network print queues and controls all print jobs. On a dedicated Web server, this service can be disabled when no printing is required.
Protected Storage	Automatic	No change	Protects storage of sensitive information, such as private keys, and prevents access by unauthorized services, processes, or users. This service is used on a dedicated Web server for smart-card logon.
Remote Access Auto Connection Manager	Manual	See comment	Detects unsuccessful attempts to connect to a remote network or computer and provides

Table-14: Recommended Service Startup Types on a Dedicated Windows 2003 Web Server			
Service Name	**Default Startup Type**	**Recommended Startup Type**	**Comment**
			alternative methods for connection. On a dedicated Web server, this service can be disabled when no VPN or dial-up connections are initiated.
Remote Access Connection Manager	Manual	See comment	Manages VPN and dial-up connection from the Web server to the Internet or other remote networks. On a dedicated Web server, this service can be disabled when no VPN or dial-up connections are initiated.
Remote Desktop Help Sessions Manager	Manual	Disabled	Manages and controls Remote Assistance. On a dedicated Web server, this service can be disabled. Use Terminal Services instead.
Remote Procedure Call (RPC)	Automatic	No change	Serves as the RPC endpoint mapper for all applications and services that use RPC communications.
Remote Procedure Call (RPC) Locater	Manual	See comment	Enables RPC clients using the RpcNs* family of application programming interfaces (APIs) to locate RPC servers and manage the RPC name service database. This service can be disabled if no applications use the RpcNs* APIs.
Remote Registry Service	Automatic	No change	Enables remote users to modify registry settings on the Web server, provided the remote users have the required permissions. By default, only members of the Administrators and Backup Operators groups can access the registry remotely.
Removable Storage	Manual	See comment	Manages and catalogs removable media, and operates automated removable media devices, such as tape auto loaders or CD jukeboxes. This service can be disabled when removable media devices are directly connected to the Web server.

Table -14: Recommended Service Startup Types on a Dedicated Windows 2003 Web Server

Service Name	Default Startup Type	Recommended Startup Type	Comment
Resultant Set of Policy Provider	Manual	No change	Enables a user to connect to a remote computer, access the Windows Management Instrumentation (WMI) database for that Web server, and then either verify the current Group Policy settings or check the settings before they are applied.
Routing and Remote Access	Disabled	No change	Enables LAN-to-LAN, LAN-to-WAN, VPN, and NAT routing services.
Secondary Logon	Automatic	No change	Allows you to run specific tools and programs with different permissions and user rights than the default permissions and user rights of the account under which you logged on.
Security Accounts Manager	Automatic	No change	A protected subsystem that manages user and group account information.
Server	Automatic	No change	Provides RPC support, file sharing, print sharing, and named pipe sharing over the network.
Shell Hardware Detection	Automatic	No change	Provides notification for AutoPlay hardware events.
Smart Card	Manual	No change	Manages and controls access to a smart card that is inserted into a smart card reader attached to the Web server.
Special Administration Console Helper	Manual	No change	Allows administrators to remotely access a command prompt by using Emergency Management Services. This service can be disabled when Emergency Management Services is not being used to remotely manage the Web server.
System Event Notification	Automatic	No change	Monitors system events and notifies subscribers to the COM+ Event System of these events.
Task Scheduler	Automatic	No change	Provides the ability to schedule automated tasks on the Web server.
TCP/IP NetBIOS Helper Service	Automatic	No change	Provides support for the NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution for clients.
Telephony	Manual	See comment	Provides Telephony API (TAPI) support of client programs that control telephony

Table-14: Recommended Service Startup Types on a Dedicated Windows 2003 Web Server

Service Name	Default Startup Type	Recommended Startup Type	Comment
			devices and IP-based voice connections. On a dedicated Web server, this service can be disabled when TAPI is not used by applications.
Telnet	Manual	Disabled	Enables a remote user to log on and run applications from a command line on the Web server. To reduce the attack surface, disable Telnet unless it is used for remote administration of branch offices or of Web servers that have no keyboard or monitor directly attached (also known as *headless* Web servers). Because Telnet traffic is plaintext, Terminal Services is the preferred method for remote administration.
Terminal Services	Manual	See comment	Allows multiple remote users to be connected interactively to the Web server, and provides display of desktops and run applications. To reduce the attack surface, disable Terminal Services unless it is used for remote administration of branch offices or headless Web servers.
Terminal Services Session Directory	Disabled	No change	Enables a user connection request to be routed to the appropriate terminal server in a cluster.
Themes	Disabled	No change	Provides user-experience theme management.
Uninterruptible Power Supply	Automatic	No change	Manages an uninterruptible power supply (UPS) that is connected to the Web server by a serial port.
Upload Managers	Manual	See comment	Manages the synchronous and asynchronous file transfers between clients and servers on the network. Driver data is anonymously uploaded from these transfers and then used by Microsoft to help users find the drivers they need. The Driver Feedback Server asks for the permission of the client to upload the hardware profile of the Web server and then search the Internet for information about how

Table-14: Recommended Service Startup Types on a Dedicated Windows 2003 Web Server			
Service Name	**Default Startup Type**	**Recommended Startup Type**	**Comment**
			to obtain the appropriate drivers or how to get support. To reduce the attack surface, disable this service on dedicated Web servers.
Virtual Disk Services	Manual	No change	Provides software volume and hardware volume management service.
Volume Shadow Copy	Manual	No change	Manages and implements volume shadow copies that are used for backup and other purposes. This service can be disabled when volume shadow copies are used on the Web server.
WebClient	Disabled	No change	Enables Windows-based programs to create, access, and modify Internet-based files.
Windows Audio	Disabled	No change	Manages audio devices for Windows-based programs.
Windows Image Acquisition (WIA)	Disabled	No change	Provides image acquisition services for scanners and cameras.
Windows Installer	Manual	No change	Adds, modifies, and removes applications that are provided as a Windows Installer (.msi) package.
Windows Management Instrumentation	Automatic	No change	Provides a common interface and object model to access management information about the Web server through the WMI interface.
Windows Management Instrumentation Driver Extensions	Manual	No change	Monitors all drivers and event trace providers that are configured to publish WMI or event trace information.
WinHTTP Web Proxy Auto-Discovery Service	Manual	See comment	Implements the Web Proxy Auto-Discovery (WPAD) protocol for Windows HTTP services (WinHTTP) and enables an HTTP client to automatically discover a proxy configuration. On dedicated Web servers, this service can be disabled
Wireless Configuration	Automatic	See comment	Enables automatic configuration for IEEE 802.11 adapters. On dedicated Web servers without wireless

Table-14: Recommended Service Startup Types on a Dedicated Windows 2003 Web Server

Service Name	**Default Startup Type**	**Recommended Startup Type**	**Comment**
			network adapters, this service can be disabled.
WMI Performance Adapter	Manual	See comment	Provides performance library information from WMI providers to clients on the network. On dedicated Web servers that do not use WMI to provide performance library information, this service can be disabled.
Workstation	Automatic	No change	Creates and maintains client network connections to remote servers.

* Some changes have been made in the services and its default startup type in Windows 2003 R2.