

IIS best practices

Explanation

The IIS installation risks and their remedies have already been discussed. Now we'll look at some security risks to the IIS servers. You'll concentrate on an operational IIS Web server and its challenges. A fictitious AllWebRequest online shopping site is used as an example to illustrate the scenarios.

The AllWebRequest online shopping site sells bicycles and bicycle accessories. This Web site is hosted on a Windows Server 2003 IIS 6.0 implementation. The scripting is done with ASP.NET pages that are written in C# language. The users use a third-party e-commerce gateway for checkout facilities. Basic authentication is used as the preferred authentication method to implement the e-commerce shopping site.

The first risk is the non-HTTP requests that are directed to the IIS server. You need to disable all non-HTTP and HTTPS data. You don't need to open any ports other than port 80 and 443 for this public Web site. (Intruders can penetrate the system if other ports are open. For example, intruders can mimic sales orders or purchase orders if you open port 21, which is used for e-mail access. If an intruder writes an e-mail from port 21, it can be forwarded to the third-party e-commerce gateway to transfer funds to bogus accounts. The third-party e-commerce gateway would authorise the transaction since it arrived from your servers. The remedy for this is to enable the ICF or use the corporate firewall to filter all non-HTTP and non-HTTPS data to the server.)

The next risk to the AllWebRequest IIS server is the authentication mechanism. The Web site is hosted internally within the enterprise. However, the payment e-commerce gateway is an external entity. Therefore, there are two risks here. The online user employs clear text to transfer credentials to the IIS server. The IIS server also transmits clear-text payment details to the payment gateway. Both of these transactions are risks to the enterprise. An intruder can intercept either of these transmissions with the help of packet-snooping software. Therefore, you need to encrypt both these communication lines with SSL.

You should also be careful of the file structure of the AllWebRequest online shopping site. The third-party e-commerce gateway broker is an executable or a DLL. Therefore, you need to assign execute permission at the Web site level to proceed to the payment gateway. You need to assign execute permission to the entire root directory, if you mount this DLL or .EXE on the root directory. This isn't a recommended practice. The complete root directory would have execute access, which isn't a healthy scenario for the IIS server. You should minimise write and execute access as much as possible on IIS servers. The best way to get around this problem is to copy the DLL or exe to a new directory and assign only execute access to that new directory (and leave the root directory with read access).

You also need to factor in the ASP.NET scripting manipulations (ASP.NET code can be scripted in a malicious way to harm the IIS 6.0 servers). This is another risk to the enterprise. You shouldn't use any

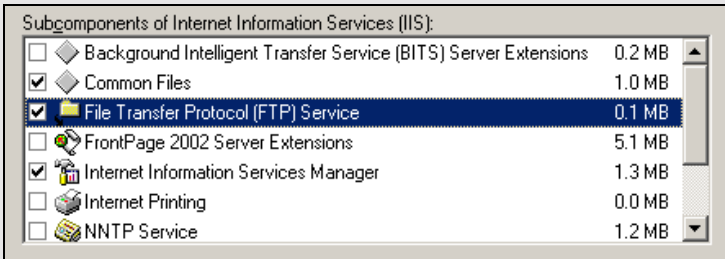
HTTP GET methods to post data to the server in your client-side scripting. This displays the form tag information on the URL box of the browser. A clever intruder can piece together a malicious request by observing these requests. Therefore, you should use the HTTP POST form method to direct HTTP requests to the IIS server. The intruders can also pass JavaScript `<script> code </script>` tags in the URL string. These are picked up by the URLScan algorithm in IIS 6.0. You should also be careful of SQL injection issues with IIS. This problem is similar to that of the previous JavaScript mechanism. The key difference is that the code fragments are SQL database commands. Hackers generate these commands by observing HTTP GET entries to the Web site. (HTTP GET posts are appended to the URL query string and are displayed to the user.

The user can change the URL query string and re-post the data to observe a different outcome of the same Web page.) Therefore, you should never display database table names in the query string. You can stop these SQL injections with URLScan and by configuring the SQL database to best practices. (URLScan is an algorithm that every oncoming request is subject to in IIS 6.0. It scans the URL query string for invalid characters and `<Script>` tags and filters them from the query string.) You can also minimise query string manipulations by assigning execute permissions to a small number of directories. Some other IIS best practices are:

- **Log on with the fewest credentials.** Don't log on as Administrator to the IIS servers. This enables the servers to configure software with fewer credentials. Use the RunAs command, if you want to run IIS Manager as an administrator.
- **Disable unwanted services in IIS 6.0.** Disable the FTP, NNTP or SMTP services that aren't used on the server. This saves valuable resources that can then be dedicated to the WWW service.
- **Keep virus scanners up-to-date.** A virus scanner compares its virus signature database with file system folders. This signature database needs to be updated regularly, since new viruses are introduced frequently. Therefore, you need to make sure these signature databases are up-to-date in order to protect your IIS and Web site files from viruses.
- **Keep all software patches up-to-date.** Windows Server 2003 comes with Auto Update version 1.0. This informs server administrators when new patches become available.

Do it!

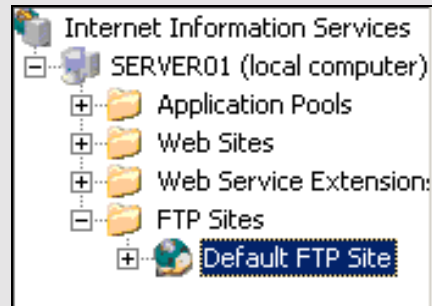
B-4: Installing FTP

Here's how	Here's why
1 Place the Windows Server 2003 CD-ROM in your CD-ROM drive	(If necessary.) You'll install and test an FTP server.
2 Click Start and choose Control Panel, Add or Remove Programs	
3 Click Add/Remove Windows Components	
4 From the Components list, select Application Server Click Details	If necessary.
5 From the Subcomponents of Application Server list, select Internet Information Services (IIS) Click Details	
6 Check File Transfer Protocol (FTP) Service , as shown	
	
Click OK	To close the dialog box.
Click OK	To close the dialog box.
Click Next	
7 Click Finish Close the Add or Remove Programs window	When the installation is complete.
8 Click Start and choose Administrative Tools, Internet Information Services (IIS) Manager	<i>Cont'd</i>

9 In the left pane, expand your server

Expand FTP Sites

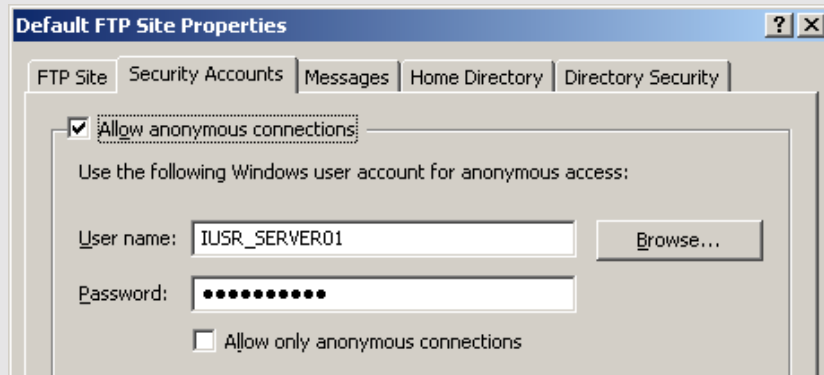
Click **Default FTP Site** as shown



10 Right-click **Default FTP Site**

Choose **Properties**

11 Activate the Security Accounts tab, as shown



Notice that this service uses the same user account for anonymous access as the Web server.

Clear **Allow anonymous connections**

Observe the warning dialog box

12 Click **Yes**

To continue. Be aware that the Windows Server 2003 implementation of FTP can't be configured to use SSL.

13 Activate the Directory Security tab

Notice that the only option here is to restrict or allow access based on IP addresses.

Cont'd

14 Click the Home Directory tab	Notice that here you can control whether the data can be uploaded or downloaded through this site. By default, write access is disabled.
Check Write	
15 Click OK	To close the default FTP Site Properties dialog box.
Close the Internet Information Services (IIS) Manager window	
16 Start Internet Explorer	
17 In the Address bar, type ftp://<ComputerName>	Where <ComputerName> is the name of your server.
Press ⓔ	Since anonymous access to this FTP site has been disabled, you're prompted for a user name and password. The user name and password given must have at least read NTFS permission to the FTP files.
18 In the User name box, enter Administrator	
In the Password box, enter Password!	
Click Log On	The window that opens is blank, because there are no files in the FTP site yet. You can copy files into and out of this window by using cut and paste from Windows Explorer and other file management applications.
19 Close Internet Explorer	

Securing FTP, NNTP and SMTP

Explanation

Now you'll investigate how to secure other IIS 6.0 components – specifically, FTP, NNTP and SMTP.

Securing FTP

The File Transfer Protocol (FTP) is a valuable component of IIS 6.0. FTP is used to swap or share files between servers and clients. This could be a dangerous practice for businesses with sensitive information. Most large organisation firewalls block FTP access. Unblocked firewalls are unhealthy for an organisation. For example, a disgruntled employee could use FTP to provide sensitive data to its competitors.

You can create individual accounts for each FTP user using IIS Manager. You also need to provide a username and password to initiate the FTP transfer. These credentials are passed as clear text from the client to the FTP server, which isn't secure for the enterprise. An intruder can 'sniff' these packets and obtain the credentials. The intruder can use these credentials to download sensitive information or upload malicious content to the server.

So, how do you secure FTP communication? You need to implement FTP communication over a secure channel like VPN. VPNs use the Point-to-Point Tunneling Protocol (PPTP), or Secure Internet Protocol (IPSec), to encrypt data and facilitate secure FTP communication. You can also use SSL encryption on WebDAV-supported directories for the same purpose.

Securing NNTP

The Network News Transfer Protocol (NNTP) is another important component of IIS 6.0. The default settings enable any user to connect to the newsgroups without any authentication process. Users can ask to view all newsgroups and subsequently subscribe to them anonymously. In some cases, you need to restrict access to the newsgroups to protect sensitive information. You can increase security on your NNTP implementation by:

- **Enabling basic authentication or integrated Windows authentication on the NNTP Service.** You need to create user accounts and add them to appropriate groups initially. Then, you grant access to the correct News folder directories to enable authentication. You must be careful regarding the local service account that NNTP uses. This account has to be granted access to the complete NNTP directories to manage the NNTP implementation correctly.
- **Restricting NNTP access by IP address.** All IP addresses have access to NNTP by default. You can configure NNTP to grant or deny access according to a specific IP address in IIS 6.0. You can also use wildcard characters to specify a subnet mask to govern access. You can use domain names, too. However, domain name wildcards need to do an additional Domain Name Service (DNS) lookup. Therefore, they're slower than the previous method.
- **Restricting the number of NNTP operators.** Operators are the administrators of the NNTP service. Windows Server 2003 enables all

the users in the Administrator group as NNTP operators. You need to configure this setting to prevent all Administrator group access. You should let only a small number of operators manage the NNTP service.

- **Using SSL to encrypt the communication.** You can also use SSL at the server and the client. The SSL certificate needs to be installed at the server. The client newsgroup reader (for example, Outlook Express) should support SSL communication to facilitate this.

Securing SMTP

The Simple Mail Transfer Protocol (SMTP) service is responsible for e-mail communication between IIS 6.0 and its clients. Most e-commerce sites use the SMTP service to send and receive purchase orders. Therefore, you need to protect your SMTP service from malicious attacks. Here are some ways to secure the SMTP service in IIS 6.0:

- **Minimise the number of operators that can manage the SMTP service.** This is similar to NNTP service operators. You need to enable a small team, or a designated Windows account group, to manage the SMTP operator access.
- **Use Transport Layer Security (TLS).** You can configure SMTP to use TLS on all incoming mail connections. TLS is similar to SSL. It secures the connection between the SMTP server and the mail client. However, it doesn't authenticate users to the SMTP services. You need to generate key pairs at the SMTP servers to implement TLS and share them with the incoming mail clients.
- **Restrict IP and network access.** This is similar to NNTP service IP restrictions. You can grant or deny access on an IP address or on a subnet mask.
- **Set basic authentication or integrated Windows authentication on outbound messages.** This is also similar to the NNTP implementation.

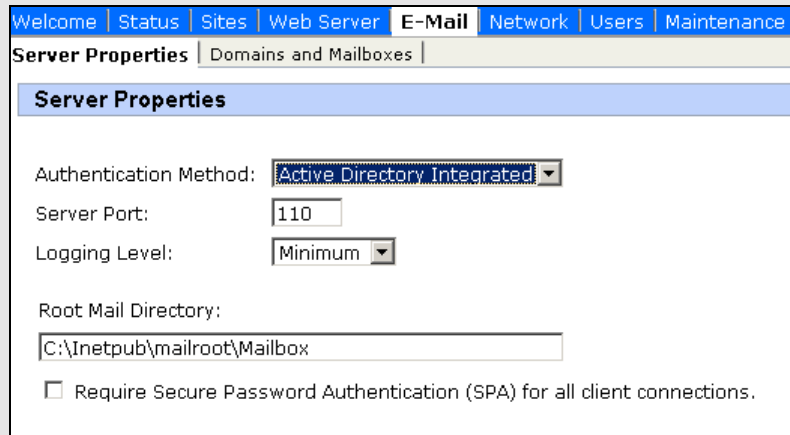
Do it!

B-5: Installing the SMTP service

Here's how	Here's why
<ol style="list-style-type: none"> 1 Place the Windows Server 2003 CD-ROM in your CD-ROM drive 2 Click Start and choose Control Panel, Add/Remove Programs 3 Click Add/Remove Windows Components 4 In the Components list, check E-mail Services 5 Click Next 6 Click Finish <p>Close the Add or Remove Programs window</p>	<p>(If necessary.) You'll install the SMTP service on your server.</p>
<ol style="list-style-type: none"> 7 Click Start and choose Administrative Tools, Web Interface for Remote Administration 8 In the User name box, enter Administrator <p>In the Password box, enter Password!</p>	<p>The Authentication dialog box appears.</p>
<p>Click OK</p>	<p>The Server Administration Web page appears, as shown.</p>
<p><i>Cont'd</i></p>	

9 Choose **E-Mail, Server Properties**

This displays the POP3 server properties, as shown.



10 Close the Internet Explorer window

11 Click **Start** and choose **Administrative Tools, Internet Information Services (IIS) Manager**

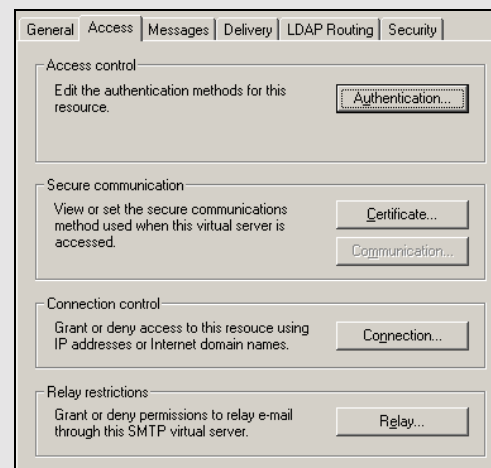
12 Expand your server

Click **Default SMTP Virtual Server**

13 Right-click **Default SMTP Virtual Server**

Choose **Properties**

14 Activate the **Access** tab, as shown



Cont'd

15 Click Relay	Notice that, by default, the Allow all computers, which successfully authenticate to relay regardless of the list above check box is checked. This allows authenticated users to relay messages. Any other options control relaying based on the source IP address of the e-mail.
16 Click Cancel	
17 Click Authentication	Notice that, by default, only the Anonymous authentication method is enabled. This means that, by default, no specific use can be authenticated to send e-mail.
18 Check Basic authentication	This allows users to authenticate and send mail.
19 Click Yes	To confirm.
20 Click OK	To close the Authentication dialog box.
Click OK	To close the dialog box.
21 Close the Internet Information Services (IIS) Manager window	

New security features in IIS 6.0

Explanation

The preceding are some ways to secure all IIS 6.0 components. IIS 5.0 and earlier versions were constantly patched by hotfixes from Microsoft. IIS was once considered one of the main security holes in the Windows architecture. This was a major deterrent to using IIS as a commercial Web server. IIS 6.0 comes with an impressive list of new security features designed to win back commercial users: advanced digest authentication, Server-gated cryptography, selectable cryptographic service providers, a configurable worker process identity, a default locked down status and a new authorisation framework.

Advanced digest authentication

Advanced digest authentication is an extension of Digest Security. Digest Security uses MD5 hashing to encrypt user credentials (user name, password and user roles). What's the purpose of MD5 hashing? Basic authentication sends the username and password details over the network medium in base-64 encoded format. These details can be easily 'sniffed' (captured with a protocol analyser) and decoded by an intruder, who could then use the credentials for nefarious purposes. The MD5 hash enhances security by applying more sophisticated, harder-to-crack cipher algorithms to deter intruders. An MD5 hash is made up of binary data consisting of the user name, password and realm. The realm is the name of the domain that authenticates the user. All of this means that Digest Security is more secure than basic authentication.

Exam tip: An MD5 hash is embedded into an HTTP 1.1 header. This is supported only by HTTP 1.1-enabled browsers. Digest or advanced digest authentication mechanisms can't be enabled if the target browsers don't

support HTTP 1.1. Internet Explorer 5.0 and later (plus recent versions of Netscape, Opera, Mozilla and other popular browsers) support HTTP 1.1,.

Advanced Digest Security takes the digest authentication model a bit further by storing the user credentials on a DC as an MD5 hash. The Active Directory database on the DC is used to store the user credentials. Thus, intruders would need to gain access to the Active Directory to steal the credentials. This adds another layer of security to protect access to Windows Server 2003 Web sites and you don't need to modify the application code to accommodate this security feature.

Exam tip: Both digest and advanced digest authentication work only on Web Distributed Authoring and Versioning (WebDAV) enabled directories. WebDAV is a file sharing protocol that's commonly used in Windows Internet-related applications. WebDAV was previously referred to as Web Folders. It's a secure file transfer protocol over intranets and the Internet. You can use WebDAV to download, upload and manage files on remote computers across the Internet and intranets. WebDAV is similar to FTP. WebDAV always uses password security and data encryption on file transfers. FTP doesn't support these.

Server-gated cryptography

Communication between an IIS Web server and the Web client uses the HyperText Transfer Protocol (HTTP). These HTTP network transmissions can easily be compromised due to their text-based messaging formats. Therefore, you need to encrypt these HTTP calls between the client and the server. Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are the most common encryption mechanisms used on Web sites. SSL/TLS enables secure communication by encrypting the communication channel with a cipher algorithm. TLS is the later version of the SSL protocol.

IIS 5.0 and earlier versions included SSL/TLS for secure communication between the Web client and the server. Server Gated Cryptography (SGC) is an extension of SSL/TLS. It uses a strong 128-bit encryption mechanism to encode the data. SGC doesn't require an application to run on a client's machine and has been available since IIS 4.0. SGC needs a valid certificate at the client Web browser, which can be encoded and decoded. A special SGC certificate is needed to enable SGC support built in to IIS 6.0. You can obtain a certificate by contacting a CA. This certificate can be added to IIS in the same way as any other certificate. IIS 6.0 supports both 40-bit and 128-bit encryption sessions. This means your old 40-bit SGC certificates are still valid in IIS 6.0. SGC is commonly used by banking and other financial institutions to protect data.

Exam tip: 40-bit SGC certificates in IIS 6.0. If you try to open an existing 40-bit SGC certificate, you might get the warning, 'The certificate has failed to verify for all of its intended purposes.' These certificates are targeted at Windows 2000 servers. Thus, you can have a valid certificate and can be misled by this warning. Windows 2000 supports only 40-bit encryption and Windows Server 2003 supports both 40-bit and 128-bit encryption.