Quickshot: Securing IIS 5.0

Technical Consulting Services
Unisys Corp.

Created October 21, 2002
Chris Mikolajewski

Version Control

Version	Date	Summary of Changes
0.9	10/21/02	Initial document created
0.9a	10/29/02	Added IIS Lockdown Wizard 2.1 to checklist
1.0	1/16/03	Final Version

Purpose

The purpose of this document is to provide a short and concise method for securely installing and configuring Internet Information Services (IIS) 5.0. It includes both pre-installation steps and the steps necessary to secure IIS after installation. The checklists are sorted by importance—the most critical steps are listed first. Various Microsoft utilities (HFNETCHK, IIS Lockdown Wizard 2.1, URLScan, etc) are essential IIS utilities that are mentioned in this checklist. These files can be downloaded from http://www.microsoft.com.

This document is tightly related to its "parent" document, QuickShot: Securing Windows 2000. The Windows 2000 recommendations should apply to all hosts running Windows 2000. Then any systems utilizing IIS should follow the guidelines in this document. This will provide the most secure system.

Tighter security always comes at the expense of convenience. The most secure system would be a host that is not attached to a network and locked in a vault. The server would be impossible to compromise, but at the same time its utility as a legitimate business tool would be minimal. This is an example of the constant trade-off between security and convenience that must be continually evaluated when implementing any type of security or hardening.

NOTE: This document is intended for advanced Windows administrators who have a full and complete understanding of the configuration changes recommended in this document. In some cases, applying the changes could cause certain systems and applications to stop functioning properly. Please understand the implications in making the changes before applying them, or test them in a non-production environment first.

IIS Pre-Installation Checklist

1. **Install Windows 2000 while disconnected from the network.**
   Until the required Service Packs and security hot-fixes are applied, Windows 2000 and IIS are not sufficiently safe from malicious attacks via the network. Install the O/S while unplugged and make sure to install the necessary service packs and critical security updates before connecting the host to the network.

2. **Install IIS on a standalone server in workgroup mode.**
   The most secure deployment option for an IIS web server is to run as a standalone server in its own workgroup. The server does not participate in any domain, which means no domain specific information (usernames, policies) will ever be stored on the web server. If joining a domain is necessary for administration reasons, install the web server in its own domain with no trusts to any other domains. If this is not possible, then install the server into the organization's standard domain. Never install IIS on a server acting as a domain controller—if the web server is compromised all of the sensitive domain information will be at risk.

3. **Repartition key content files to a different hard drive partition then the C:\ drive.**
   Many of the known attacks on IIS involve directory transversal from the content directory (by default `C:\inetpub\wwwroot`) up the directory tree to the `C:\winnt\system32` directory. There the attacker has access to any number of powerful system commands. Installing the content files on drive D:\ for example will prevent these types of attacks.

IIS Post-Installation Checklist

1. **Apply the latest patches for Windows and stay current with newly released critical security updates.**
   Microsoft continually releases new critical security updates for vulnerabilities that are discovered in IIS and its components. Once downloaded and tested on non-production systems, these updates should be installed on all affected servers in an organization.

   Windows 2000 Service Pack 3 was released in August of 2002. Install Service Pack 3 on all Windows 2000 systems along with any critical security updates that have been issued for IIS since its release.

   In some cases, their may be a technical reason not to install Service Pack 3 (i.e. an incompatibility with existing applications). If this is the case, install Service Pack 2 and ensure that the latest post-SP2 critical security updates are also applied.

   Microsoft has released a software package called Software Update Services (SUS) that makes it easier to download and deploy critical updates, critical security updates, and security roll-ups for Windows 2000, XP, and .NET Server hosts. An administrator creates an update server within the organization that automatically downloads any new updates from Microsoft. Once the administrator approves the downloaded updates, they are pushed out to all the host machines configured with the SUS client software. The SUS software and documentation can be found at the following link:

   http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp

   Use the Microsoft Hot Fix Network Checker (HFNETCHK) to easily check what service packs and updates have been applied to a system. HFNETCHK is a free tool from Microsoft that can be used to check and see what patches and hot-fixes have been applied to servers. Use this tool to verify that all the servers have had the most recent critical security updates applied.

   Subscribe to the Microsoft Security Notification Service. This is a free email notification service that Microsoft uses to send out security updates to subscribers. Whenever a new

security bulletin is posted, an email will get sent to subscribers detailing the bulletin. The link to subscribe is listed below:

http://www.microsoft.com/technet/security/bulletin/notify.asp

2. **Disable or uninstall unneeded IIS components.**
Only install the IIS components that are needed for the web server. Below is a list of all the IIS components that can be installed through Control Panel | Add/Remove Windows Components.

- Common Files
- Documentation
- File Transfer Protocol (FTP) Server
- FrontPage 2000 Server Extensions
- Internet Information Services (IIS) Snap-in
- Internet Services Manager (HTML)
- NNTP Service
- SMTP Service
- Visual InterDAV RAD Remote Deployment Support
- World Wide Web Server

To configure a "standard" Web server (ASP and static content), you only need to install the following components:

- Common Files
- Internet Information Services (IIS) Snap-in
- World Wide Web Server

By default, IIS also installs various functions and code samples that pose security risks. Delete the following virtual directories from the Default Web Site:

- Scripts
- IISHelp
- IISAdmin
- IISSamples
- MSADC (very important-this disables Remote Data Services (RDS)
- Printers

NOTE: Windows will try to re-create the Internet Printing virtual directory when the system reboots—this is because the setting is controlled by Group Policy. To resolve this, open the Group Policy MMC Snap-In and browse to Local Computer Policy | Computer Configuration | Administrative Templates | Windows Components | Printers. The "Web-based printing" policy should be set to "Disabled."

By default IIS utilizes files in the IISHelp virtual directory for its various error messages. These custom errors no longer work once the IISHelp virtual directory has been removed. To remedy this, browse to the Master Properties for the WWW Service. Under Custom Errors, select all the messages and click "Set to Default."

Also, delete the directories (and all the files in them) associated with the above virtual directories:

- `c:\inetpub\AdminScripts`

NOTE: The script files in this directory can be helpful in administering a website—copy the scripts to a different folder before deleting.

- `c:\inetpub\IISSamples`
- `c:\inetpub\Scripts`
- `c:\winnt\web\printers`

Some default asp and picture files will still be in the `C:\intepub\wwwroot` directory. Delete these files as well.

World Wide Web Distributed Authoring and Versioning (WebDAV) is an extension to the HTTP protocol that allows remote authoring and management of Web content. By default, the entire Web space of IIS is capable of responding to WebDAV requests (even though the security settings will not allow publishing by default). The WebDAV functionality is provided by the httpext.dll file. For more information on WebDAV, refer to Microsoft KB article 241520.

Most standard websites (static content and ASP code) will never need WebDAV functionality and therefore can safely disable it. IIS Lockdown Wizard attempts to "disable" WebDAV by apply a deny EXECUTE ACE for EVERYONE on the httpext.dll file. Unfortunately, this will still allow PUT and DELETE WebDAV requests to execute. A new registry key was introduced with the Windows 2000 Security Rollup Package (SRP1), which was released in January 2002. These key allows an administrator to fully disable all WebDAV functionality on the IIS server. The key is as follows:

- Key: HKLM\System\CurrentControlSet\Services\W3SVC\Parameters
- Value: DisableWebDAV
- Value Type: REG_DWORD
- Value Data: 1

This key was also included in Service Pack 3. If the IIS host is running an earlier Service Pack or without the SRP1 installed, use the basic security capabilities that IIS Lockdown Wizard provides to secure WebDAV.

3. **Remove unnecessary script mappings (ISAPI extensions).**

   NOTE: This step should be done on the Master Properties of the WWW Service. The changes are then filtered down to any and all web sites running on the server.

   IIS is configured to support many different types of filename extensions, which it then parses through the various application `.dll` files. Some examples of these script mappings would be `.asp`, `.stm`, and `.htr`. By default, script mappings are installed with IIS 5.0 that allow web-based password resets and network printer installations. These are advanced features that are not typically needed for web applications. If the script mapping is not needed, it should be removed. This will protect the server against certain malicious attacks, such as buffer overflows.

   The following script mappings should be removed, leaving only `.asp` and `.asa` as valid options:

   - `.htw`
   - `.ida`

- .idq
- .cer
- .cdx
- .htr
- .idc
- .stm
- .shtm
- .shtml
- .stm
- .printer

NOTE: Installing the Microsoft .NET framework on an IIS 5.0 host will add a number of script mappings to the Default Web Site. They should not be deleted.

4. **Ensure IIS logging is enabled.**

   NOTE: This step should be done on the Master Properties of the WWW Service. The changes are then filtered down to any and all web sites running on the server.

   Ensure IIS logging is turned on (it is by default), and make sure the following values are being logged using the **W3C Extended Log File Format**:

   - Date
   - Time
   - Client IP Address
   - User Name
   - Server IP Address
   - Server Port
   - Method
   - URI Stem
   - URI Query
   - Protocol Status
   - Time Taken
   - User Agent

   NOTE: All fields except the "**Time Taken**" field is enabled by default.

5. **Tighten the IIS application level permissions.**

   NOTE: This step should be done on the Master Properties of the WWW Service. The changes are then filtered down to any and all web sites running on the server.

   For an end-user to access resources on an IIS server, they must traverse through various levels of authentication before they are granted access to the resources. These "authentication gateways" are as follows (in descending order):

   - IIS IP address and domain name restriction
   - IIS authentication (anonymous, basic, integrated Windows, etc)
   - IIS application level permissions
   - NTFS ACLs

This step secures the default IIS application level permissions, which can be configured through the Internet Services Manager. Click on each web site and choose **Properties**. The permissions are set under the **Home Directory** tab. For every directory in your web site, you should enable "**Log Visits**" and disable "**Index this resource**." The configuration of the remaining settings really depends on how the web site will be used. For directories with static content, the only IIS permission needed is the "**Read**" permission.

The **Execute Permissions** setting also needs to be reviewed. This setting controls the execution of applications within the directory. Make sure you understand the implications of enabling either "**Scripts**" or "**Scripts and Executables**" before enabling access.

6. **Install the IIS Lockdown Wizard 2.1.**
IIS Lockdown is a utility from Microsoft that makes it easy to apply a large number of security settings to IIS web servers. The latest version, 2.1, has a set of server roles the installer can choose from. They cover a wide range of Microsoft products (Exchange, Biztalk, FrontPage Server Extensions, etc.). IIS Lockdown Wizard takes this information and applies a specific set of security settings that will still allow the server to function in its role. For most web servers, choosing the "Dynamic Web Server (ASP Enabled)" role will apply the appropriate security settings.

Please note—all of the actions taken by the IIS Lockdown Wizard can also be accomplished manually. The benefit from using the Wizard is it can automate some tedious tasks, such as setting ACLs on multiple files. We also need to run the Wizard because it installs the URLScan ISAPI filter, which provides IIS with another level of security.

Install the IIS Lockdown Wizard using the following configuration guide:

- Choose Dynamic Web Server (ASP Enabled) as the server role. Click the box to view template settings.
- Disable Web Distributed Authoring and Versioning (WebDAV).
- Set file permissions to prevent anonymous IIS users from writing to content directories
- Set file permissions to prevent anonymous IIS users from running system utilities
- Install URLScan filter on the server

What the IIS Lockdown Wizard actually does to the system

To disable WebDAV, the wizard sets a deny EXECUTE ACE on the httpext.dll file for EVERYONE. This disables most of the WebDAV functionality, but still allows PUT and DELETE requests in IIS. Follow the last steps in Item 2 of the Post-Install Checklist to fully disable WebDAV.

IIS Lockdown Wizard creates two local groups called "**Web Anonymous Users**" and "**Web Applications**." It adds the **IUSR_Computername** user to the "**Web Anonymous Users**" group, and adds the **IWAM_Computername**" user to the "**Web Applications**" group. It uses these groups to assign the NTFS file permissions to the C:\WINNT and C:\INETPUB\WWWROOT directory. Use these groups when applying file permissions to the anonymous user accounts.

Using these two local groups, IIS Lockdown Wizard sets a deny FULL CONTROL ACE on all .EXE and .COM files in the C:\WINNT directory for both the Web Anonymous and Web Applications group. It also sets the same ACE on the C:\inetpub\wwwroot directory.

URLScan is an ISAPI filter that is installed on the web server. It intercepts all web requests before IIS processes them and can be configured to accept or deny specific HTTP requests. URLScan intercepts malicious requests before they reach the server so IIS does not process them. Using the Dynamic Web Server (ASP Enabled) template, URLScan will deny all HTTP requests except GET, HEAD, and POST, and will only allow certain types of files to be requested, such as .ASP, .JPG, and .GIF.

7. **Disable the Indexing Service.**
   The Microsoft Indexing Service continually runs in the background and indexes all of the documents on a server. These documents can include website files, which could expose sensitive code. If you do not use the Indexing Service, stop and disable it from the Services Control Panel. Also check each Web Site and make sure that "Index this resource" checkbox is not checked under Internet Services Manager | Web Site Properties | Home Directory.

8. **Secure ODBC operation.**
   ODBC is the most commonly used method for accessing databases on a Windows system. Unfortunately, ODBC inherently allows for DOS commands to be embedded in ODBC calls. Several vulnerabilities have arisen that demonstrate how DOS commands could be chained together in ODBC queries, resulting in the invocation of CMD.EXE. Microsoft provides a mechanism to prevent ODBC calls from invoking DOS commands by changing the Sandbox Mode from 2 to 3 in the registry. Further information can be found in the Microsoft KnowledgeBase article Q239482.

   - Key: HKLM\Software\Microsoft\Jet\4.0\Engines
   - Value: SandboxMode
   - Value Type: REG_DWORD
   - Value Data: 3 (This is from the default value of 2.)

9. **Update Root CA certificates.**
   Root certificates allow for a secure communication path with the web server. By default Windows 2000 installs a large number of root certificates on the server. You can view this list by using the Certificates MMC snap-in and selecting "Trusted Root Certification Authorities." Remove any certificates that you do not trust—basically if you do not know the name of the company who issued the certificate then you should not trust it. Delete the certificates you do not trust.

References

"SANS/FBI Top 20 List – The Twenty Most Critical Internet Security Vulnerabilities (Updated);" version 2.6; October 1, 2002; http://www.sans.org

"From Blueprint to Fortress: A Guide to Securing IIS 5.0;" John Davis; June 2001; http://www.microsoft.com

"Secure Internet Information Services 5 Checklist;" Michael Howard; Windows 2000 Security Team; June 29, 2000; http://www.microsoft.com

"10 Steps to Better IIS Security;" Russ Cooper; http://www.ntbugtraq.com

“Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0;” William E. Walker IV; National Security Agency; version 1.1.4; June 19, 2001