



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Securing Windows and PowerShell Automation (Security 505)"
at <http://www.giac.org/registration/gcwn>

Securing Microsoft Internet Information Server 5.0 Using the Windows 2000 Internet Server Security Configuration Tool

George M. Garner Jr.

August 15, 2000

1. Introduction.

Internet Information Server (IIS) 5.0 represents another milestone in Microsoft's effort to transform its Windows 2000 operating system into an Internet applications platform. IIS 5.0 is more fully integrated with the operating system than its predecessors. As such it leverages operating system services to provide ease of setup, networking, fault tolerance, centralized management, and distributed applications. IIS 5.0's integration with the operating system is nowhere more evident than in IIS's use of Windows 2000 security. In a very real sense, IIS 5.0 security is Windows 2000 security. Windows 2000 supports a rich security feature set, including kerberos, NTLM and certificate authentication. However, the very richness of its feature set make proper security configuration difficult. There is a vital need for tools that will automate the process of securing Windows 2000 based on configurable policies. Windows 2000 provides many tools for this purpose. However, it does not provide any tools dedicated to securing the operating system for use as a web application platform.

Recently, Microsoft has released the Internet Server Security Configuration Tool for public comment. The tool is still a little rough and does not work consistently. However, it is important to understand and comment on this tool to give Microsoft guidance on its further development.

The following paragraphs will briefly describe how to use the tool to configure and implement an IIS Security Template. Note that this article is not intended to be a step-by-step overview. It assumes that the reader already has a basic familiarity with Windows 2000 and security templates. References are provided to allow the reader to delve more deeply into what the tool does (and does not) do.

2. Using the Windows 2000 Internet Server Security Configuration Tool to Create a Security Template.

2.1. Installing the Internet Server Security Configuration Tool.

Version 1.0.20 of the IIS Server Security Template Configuration Tool (the "Tool") may be downloaded from the Microsoft [web site](#). To install the Tool, unzip the contents of the file iislock.exe into a folder that is accessible from the computer that you wish to configure. Unzipping the Tool creates a "Tools" directory that contains two subdirectories, one named "DataEntry," and the other named "Engine." The "DataEntry" subdirectory contains a collection of web pages that provide the user interface for the Tool. The "Engine" subdirectory contains a collection of scripts and executables that are used to apply the policies that have been configured using the user interface. The

“Engine” subdirectory also includes a Windows 2000 security template, hisecweb.inf, which may be downloaded separately from the [Microsoft web site](#).

Nota Bene: The “security template” created by the Tool is not the same thing as a Microsoft Windows 2000 security template that. The Tool does not modify the included hisecweb.inf. To review and edit hisecweb.inf, you need to use a Microsoft Management Console (MMC) snapin called the Security Configuration Editor (SCE). You may create an IIS security template using the Tool. However, do *not* use the Tool to apply security settings until you have reviewed and modified the contents of hisecweb.inf to conform to your company’s security policy.

Since the Tool includes executable files that configure sensitive security policies, you may wish to place the Tool into your “Program Files” directory and restrict the Tool for use by Administrators using NTFS file permissions. You also may wish to install shortcuts to the Tool’s default web page and to a command console set to the “Engine” subdirectory. This will make it easier to locate and use the Tool’s data entry and configuration components.

Next, open a command console and set the current path to the location of the “[Engine](#)” subdirectory that you have just installed. Type “regsvr32 iissecuritywiz.dll” into the console and press enter. This will register a [COM+](#) component that performs administrative checks and service manipulation.

2.2. Configuring and Creating an IIS Security Template.

2.2.1. Known Limitations.

Before you begin, review your company’s security policy. The Tool provides a limited set of functions to implement this policy. But it does not provide a comprehensive recommendation as to what this policy should be. Also before you begin, read the “ReadMe” file that accompanies the tool. The “ReadMe” file contains information on how to use the Tool and the command line utilities that accompany the Tool. More importantly, the “ReadMe” file contains information on the limitations of the Tool. Do not use the Tool to apply an IIS security template until you have reviewed and understand these limitations.

Here are some of the Tool’s most notable limitations:

- The Tool does not configure all common applications nor address many common web scenarios.
- The Tool cannot configure (properly) a multi-homed server.
- While the tool may be used to configure a remote server, the SCE policy will be deployed to the *local* server.
- The Tool is best used to configure a stand-alone server, rather than the member of a domain. You can use the Tool to configure a server that is the member of a Windows 2000 domain, however, the *domain* security policy may override the local security policy configured by the Tool.

- By default, the Tool will create and deploy an IPSec policy that essentially blocks all network traffic to your computer except for traffic over tcp port 80. Other ports may be opened, depending on how you configure the IIS security template, however, if you are not careful, you may render your server inaccessible except from the local console.
- The Tool envisions a fresh install of Windows 2000 Server and IIS 5.0. If you have already made significant changes to IIS or the security policy on your server, the Tool may not function properly.
 - The Tool will not reinstall IIS components that you have already deleted. Also, the Tool will look for the “Default Web Site” and the “Admin Web Site” under those names. It will not operate properly if you have renamed those sites.
 - The Tool will create an IPSec policy named “Secure Web” on the local server. However, the Tool will not replace a policy named “Secure Web” if one already exists.

The “ReadMe” file is located in the “[Tools](#)” directory referred to [at the beginning of this article](#). The “ReadMe” file also may be opened from a link on the Tool’s [home page](#).

2.2.2. Configuring an IIS Security Template.

Now that you have installed the Tool, you can proceed to create a security template for your web server. To create a security template, open the file “default.htm,” located in your “DataEntry” subdirectory, into Explorer 5. This will display the Tool home page, as can be seen in [Figure 1](#).

The Tool home page consists of two frames. The left frame contains links to the Tool home page, to the “ReadMe” file for the tool, to the IIS security template configuration form, to the [Microsoft Security](#) web site and to version and legal information about the tool. The right frame contains a (non-functional) list of the same links, plus a brief explanation of how to use the Tool.

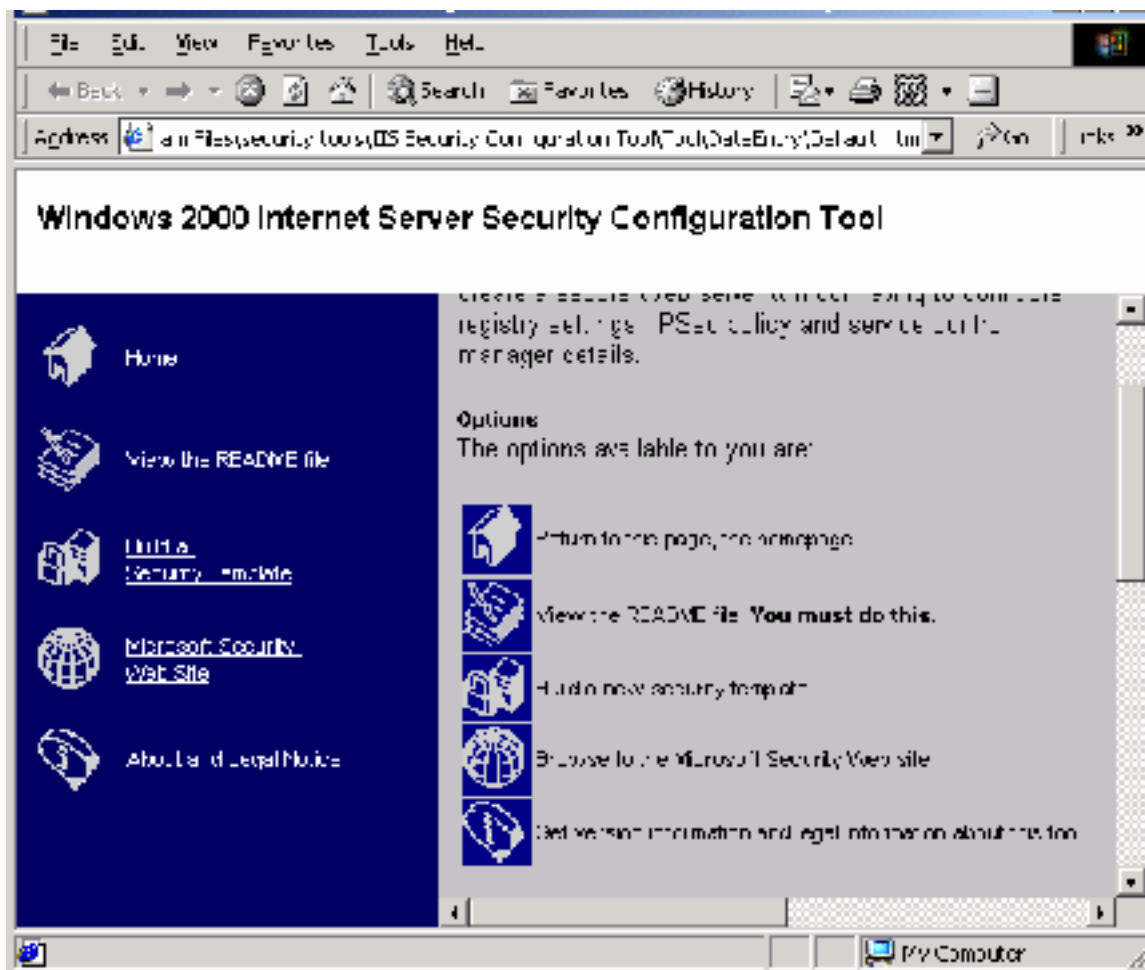


Figure 1. The IIS Security Configuration Tool Home Page.

Be sure to read the “ReadMe” file before you proceed further. Do not use the Tool to apply an IIS security template until you have reviewed and understand the Tool’s [known limitations](#).

To configure an IIS security template, click on the link in the left frame entitled “Build a Security Template.” The Tool’s template configuration form ([Figure 2](#)) will be displayed in the right frame.

© SANS Institute

Nota Bene: You still will need to select this option if the root of your web server or any of its virtual web sites are linked to a network file share that is located on a Windows NT 4.0 or Samba server since these do not support Microsoft Networking over port 445. You also will be required to “weaken” your server’s security policy in a number of other significant ways. The hisecweb.inf security template that is supplied with the Tool is designed to be compatible with these so-called “down-level” systems.

2.2.2.2. Remote administration using the Admin Web Site.

The second option is to “Remotely administer this computer over the Web.” You should select this option if you intend to administer your web server remotely over Internet. You also should select this option if you intend to administer your web server remotely over the local intranet and intend to disable the Server service.

By default, this web site is named “Admin Web Site” and is configured to use an a-standard port (not port 80). If you select this option, the Tool will look for the administrative web site under this name and attempt to determine the port over which the server is listening. If the Tool finds the administrative web site, the Tool will permit traffic over this port in its IPsec policy.

The administrative web site is an attractive alternative for anyone who needs to administer a web server remotely over the Internet. The administrative web site continues to function even with the server service disabled on the server. However, potential hackers almost certainly will locate this site due to its use of an a-standard TCP/IP port. It is likely to become the target of attack. If you select this option you should protect the administrative web site by requiring Secure Sockets Layer/Transport Layer Security (SSL/TLS) encryption plus some form of authentication. Both basic and certificate based authentication work well over the Internet and do not require the Microsoft browser. Over the local intranet, Integrated Windows authentication (Kerberos plus NTLM) also may be used. On a multi-homed server, you can block access to the administrative web site from the Internet while still using the site’s administrative functions from the local intranet. The Tool does not support multi-homed web servers, however, [as has already been noted](#).

Note that the administrative web site is not the same thing as the “IISAdmin” virtual folder installed under the default web site. If you are an operator for an individual virtual web site, you can still administer that site using the IISAdmin folder even if you have deleted the administrative web site. Note also that the Tool does not require SSL encryption on the administrative web site, nor does it check to see if SSL already is required. Neither does the Tool require authentication on the administrative web site or check to see if the site has been configured to require authentication. The Tool does not even allow traffic over port 443 (SSL) unless [option 6](#), below, is selected. If you leave this option unselected, the Tool will not remove the administrative web site.

2.2.2.3. Use this server as a File Transfer Protocol server (FTP).

FTP is still a very popular protocol for transferring files anonymously over the Internet. Every time that I receive an alert from the manufacturer of my anti-virus software, I download the new virus definitions over the Internet using the FTP protocol. Most experts will recommend as a general rule that you not use your web server to host other Internet services such as FTP, SMTP, POP3 or NNTP. However, this may not be feasible for many small to mid-sized businesses. Many companies are consolidating their servers as they upgrade their servers to Windows 2000. Windows 2000 scales more easily than Windows NT 4.0 did and Personal Computer (PC) based servers have increased dramatically in their computing power. Reducing the number of servers in an operation can have a significant positive impact on the total cost of ownership (TCO). Select this option if you intend to offer the FTP service from your web server. By default, the Tool disables the FTP service and closes ports 20 and 21 in the IPsec policy generated by the Tool. If you select this option, the Tool will enable the FTP service and will permit traffic over ports 20 and 21 in the IPsec policy.

Note that the Tool does not otherwise attempt to secure the FTP service. For more information on how to secure a Windows 2000 FTP server, see Jason Fossen's tract on securing [Internet Information Server](#).

2.2.2.4. Use this server as an Internet email server (SMTP, POP3).

For similar reasons as stated above for FTP, you may wish to use your web server as an email server. The email server may function as a simple SMTP relay from your internal network to your Internet Service Provider (ISP) or from your ISP to your internal mail server. Or you may want to provide both SMTP and POP3 services together from your web server. If you select this option, the Tool will enable the SMTP service and will permit traffic over port 25. The Tool cannot enable the POP3 service since Windows 2000 does not provide one. However, the Tool does not even allow traffic over port 110 in its IPsec policy. (For this reason, the presence of the term "POP3" in the label for this option is somewhat deceptive.) IMAP is another popular mail protocol. The Tool does not accommodate using your web server as an IMAP server.

As was stated above for the FTP service, the Tool does not otherwise attempt to secure the SMTP service.

2.2.2.5. Use this computer as an Internet News (NNTP) server.

If you select this option, the Tool will enable the NNTP service and allow traffic over port 119 in the IPsec policy generated by the Tool. This is not recommended. However, you may wish to select this option for the reasons stated above concerning the FTP service.

Note that the Tool does not otherwise attempt to secure the NNTP service.

2.2.2.6. Use SSL on this server.

You need to select this option if any of your server's web sites will be secured using SSL/TLS. In particular, you need to enable this option if you selected to keep the

Administrative web site under [option 2](#), above. If you select this option, the Tool will permit traffic over tcp port 443 in the IPSec policy generated by the Tool.

Note that the Tool does not install a server certificate on your server, nor does it check to see if one has been installed. The Tool also does not configure IIS to allow or require SSL/TLS, the strength of the SSL/TLS (40 or 128-bit), the type of certificate mapping that is to be used or the type of authentication that is to be used in conjunction with SSL/TLS.

For more information on using SSL/TLS with IIS 5.0, see [Internet Information Services 5.0 Technical Overview](#) and Jason Fossen's tract on securing [Internet Information Server](#). See also, Michael Howard, *Configuring SSL/TLS and Chapter 9. Practical Privacy, Integrity, Auditing, and Nonrepudiation*, in [Designing Secure Web-Based Applications for Microsoft Windows 2000](#), pp. 134-149, 247-284, respectively.

For more information on Microsoft Windows 2000 public key infrastructure, see [Cryptography and PKI Basics](#) and [Microsoft Windows 2000 Public Key Infrastructure](#). See also, Michael Howard, *Chapter 15. An Introduction to Cryptography and Certificates in Windows 2000* in [Designing Secure Web-Based Applications](#), pp. 423-469.

2.2.2.7. Use this computer as a Telnet server.

Select this option if you intend to use telnet to remotely administer your IIS server. By default, the Tool will disable the Telnet service. Disabling the Telnet service is a good idea even if you are not running IIS. Telnet is not a secure protocol and is not required to administer Windows 2000 or IIS remotely.

If you decide to enable the Telnet service, Microsoft recommends that you restrict access to the telnet service by creating a "TelnetClients" user group on your local server. Add the users to this group who are to have access to the computer using telnet. When the "TelnetClients" group exists on the local server, the Telnet service will allow only those users defined in that group to have access to the server. [Secure Internet Information Services Checklist](#). The checklist does not explain what form of authentication the Telnet service uses. Presumably it is Integrated Windows authentication (kerberos plus NTLM). However, passwords and user ids' might be transmitted using plain text! Even if you decide not to enable the Telnet service, it is still a good idea to create the "TelnetClients" user group on the local server and *not* add anyone to the group. That way, no one will be able to use telnet to access your web server *even if* the Telnet service somehow subsequently becomes enabled.

If you select this option, the Tool will permit traffic over tcp port 23 in the IPSec policy generated by the Tool.

2.2.2.8. Allow files other than static files (.txt, .html, .gif etc) and Active Server Pages to be served.

Like other web servers, IIS 5.0 is able to serve up static web pages that contain text, html and images. However, most people who use IIS use it as an application platform. ISAPI filters and Web Applications can extend IIS. Web applications are installed in the Script Map of the IIS metabase for a web site. [Active Server Pages](#) (ASP) is a common web application on the IIS platform. If you select this option, the .asp file extension will be mapped to asp.dll in the Default Web Site's Script Map. Selecting this option also allows you to select from a number of other forms of active content on the Tool configuration page.

Note that the Tool replaces the Script Map on the Default Web Site. Any associations that are not mentioned below will be removed. In particular, the Tool will remove the association between .idc files and Microsoft Data Access Components (MDAC). Microsoft recommends using Active Data Objects (ADO) for all new applications. The Tool does not configure the Script Map on web sites other than the Default Web Site. The default installation of IIS 5.0 does not install the Remote Data Service (RDS). However, this may be present if you upgraded your server from IIS 4.0, or if you (foolishly) decided to install RDS on your own. The Tool does not check to see if RDS has not been installed, nor does it remove an existing installation of RDS.

2.2.2.8.1. Internet Printing.

Select this option if you want to enable Internet Printing on the Default Web Site. Internet printing is one of the exciting new features supported by IIS 5.0. Using Internet Printing you can print to a network printer without using Microsoft Networking. For example, you can print a document on a network printer in your office from your home or while you are traveling. You can print a document through IIS using Internet Printing as a low cost alternative to faxing the document. You may wish to offer Internet Printing as a (for profit) service to your clients. "Down-level" computer systems such as Windows 9x are able to print to a shared printer using Internet Printing even if you have disabled netbios on your local intranet, or your local security policy requires NTLMv2 and Windows 2000 strong session keys.

On the other hand, Internet Printing also is relatively new and its security implications have not yet been fully appreciated. It is best to disable Internet Printing unless you have a defined need for this functionality. If you decide to enable Internet Printing, then you should protect the "Printers" virtual folder by requiring SSL and some form of authentication (e.g. basic, Integrated Windows and/or certificate authentication).

If you select this option, the Tool adds an association between .printer files and msw3prt.dll to the Default Web Site's Script Map.

Note that the Tool does not remove the "Printers" virtual folder from the Default Web Site if you do not select this option.

For more information on IIS's support for Internet Printing, see [Internet Information Services 5.0 Technical Overview](#).

2.2.2.8.2 Server Side Includes.

[Server Side Includes](#) (SSI) is intended to promote the modularity and reusability of script and html source. By simplifying html and asp code, they make a web site more easily maintainable. All of this should improve security. However, SSI has been exploited particularly when used in conjunction with Front Page Server Extensions. [KB Q165346](#). Microsoft strongly recommends that you not enable SSI on any server on which Front Page Server Extensions also are employed. In addition, you should disable the “#exec cmd” directive by editing your web server's Registry. You can completely disable #exec directives by editing the IIS metabase. For more information on editing Registry and metabase values related to the #exec command, see *Important Registry and Metabase Values for Web Applications* in Fossen, [Internet Information Server](#).

If you select this option, the Tool will add an association between .shtm, .shtml, and .stm files and ssinc.dll. The Tool does not check to see if Front Page Server extensions are installed or the #exec directive is enabled, nor does it inform you of the risks associated with enabling server side includes.

2.2.2.8.3. Remote Password Administration.

This option will add an association between .htr files and ism.dll to the Default Web Site's Script Map. IIS remote password administration is subject to a “buffer overflow” attack. See Knowledge Base (KB) Article [Q234905](#) and <http://www.eEye.com>. Variations on this attack are still being published today and some of these variations still have not been patched. See Microsoft Security Bulletin [MS00-044](#). See also Rain.Forest.Puppy's comments in the subsequent thread “[More information on MS00-044](#).” Microsoft recommends that you un-map .htr files unless you have a mission-critical reason to use the .htr functionality. [Secure Internet Information Services Checklist](#).

Note that the Tool will not remove .htr files from your web server if you leave this option unselected. However, the Tool will remove the script mapping for .htr files from the Default Web Site.

2.2.2.8.4. Index Server.

Search engines greatly increase the utility of a web server. It is much easier to find information on a specific security-related topic on the [SANS web site](#) now that SANS has added a search engine. On the other hand, a misconfigured search engine may allow intruders access to sensitive files stored on the web server. For example, a misconfigured Index Server might allow hackers to locate and download your computer's SAM database. This would not be a good thing. If you select this option, the Tool will add an association between .idq files and ida.dll and an association between .htw files and webhits.dll. The Tool also should add an association between .ida files and ida.dll,

however, this does not happen due to a bug in the script code (applysettings.js) which adds the association to .idq files twice.

Note that the Tool does not attempt to configure Index Server. If you select this option, you need to manually configure Index Server to ensure that the proper folders are being indexed, that the proper NTFS file permissions have been placed on the indexed (and non-indexed) folders and that only the appropriate users have access to the web sites search engine. For more information on securing Microsoft Index Server, see Jason Fossen, [Internet Information Server](#).

2.2.2.9. Keep the web samples.

IIS 5.0 comes with a number of sample applications that illustrate its features. By default, these samples are located in the IISSamples folder on the Default Web Site. Many of these sample applications may be exploited to compromise your web site. These sample applications should never be deployed on a production server.

If you select this option, the Tool does nothing. If you do not select this option, the Tool displays a notice that this feature has not yet been implemented.

2.2.3. Creating an IIS Security Template.

Now that you have configured your IIS security template, you are ready to create the template. To generate the template, click “Create Template” on the Tool’s [template configuration form](#). A confirmation dialog will appear asking if you really want to create the IIS template. The confirmation dialog is displayed in [Figure 3](#).

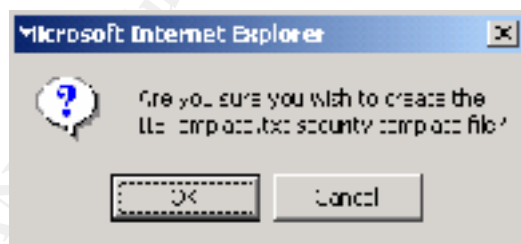


Figure 3. IIS Security Template Confirmation Dialog.

Click “OK.” A second confirmation dialog will appear advising you that you are about to see a warning that an ActiveX control may be unsafe. This is a benign warning that results because the Tool uses a FileSystem Object to create the file “IISTemplate.txt.” The second confirmation dialog is displayed in [Figure 4](#).

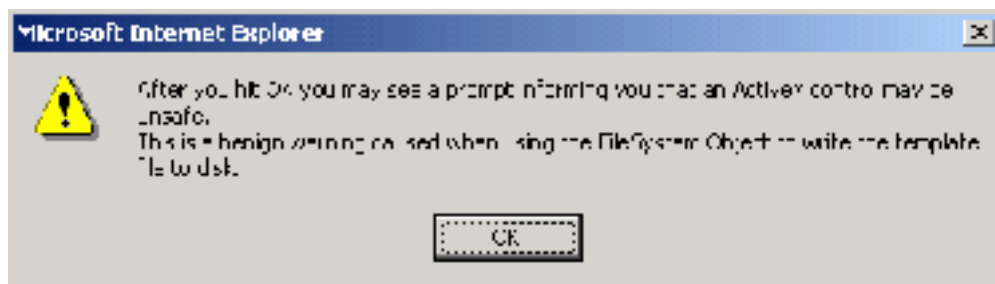


Figure 4. Warning about unsafe ActiveX control warning.

Click “OK” again and you will see an Internet Explorer dialog with the warning that was [just mentioned](#) about an unsafe ActiveX control. The dialog is displayed in [Figure 5](#).

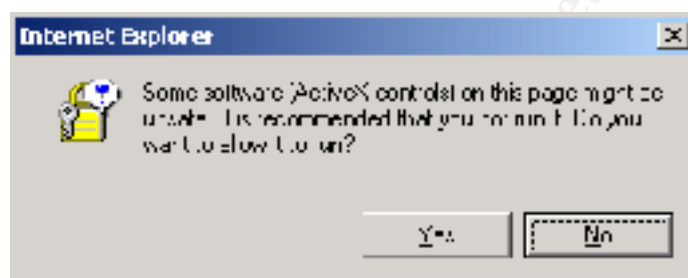


Figure 5. Unsafe Active X Control warning.

Click “OK” yet again and you will see a dialog confirming that the file “IISTemplate.txt” has been created. This dialog is displayed in [Figure 6](#).

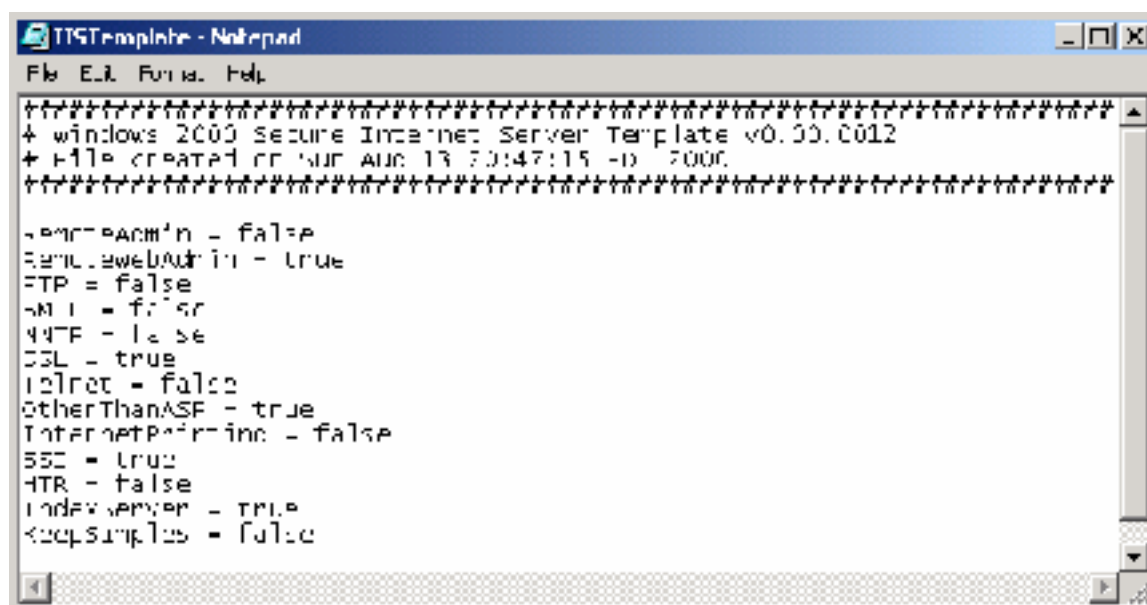


Figure 6. Confirmation dialog.

The file “IISTemplate.txt” will appear on your desktop.

There is an edit control on the [IIS security template configuration form](#) labeled “Template Name.” The default name is “IISTemplate.txt,” however you may enter any valid file and path name. To configure your server, you will need to place this file in the “[Engine](#)” subdirectory that you created when you installed the Tool. You may enter the path to this directory into the text box if you like. If the path to this directory is long, the Tool does not help you find the path.

The IIS security template that the Tool creates is a simple text file with a series of symbol-value pairs, separated by an equals sign. The contents of an IIS security template are displayed in [Figure 7](#).



```
#####
+ windows 2000 Secure Internet Server Template v0.00.0012
+ File created on WED AUG 13 20:47:15 -D 2000
#####

+SecAdmin - false
+SecWebAuthn - true
+FTP - false
+M1 - false
+M2 - false
+SSL - true
+IsNet - false
+OtherThanASF - true
+InternetPrinting - false
+SSC - true
+ATR - false
+IndexServer - true
+SecSamples - false
```

Figure 7. Listing of IISTemplate.txt.

When the Tool implements a template, the default behavior is to look for “IISTemplate.txt” in the “[Engine](#)” subdirectory. You can change this behavior from the command line by specifying a different path or file name. Or you can drag IISTemplate.txt from your desktop to the “[Engine](#)” subdirectory. If you drag IISTemplate.txt into your “[Engine](#)” subdirectory and then decide to modify the template, be sure to drag the new version of IISTemplate.txt into the “[Engine](#)” subdirectory, or the Tool will not implement the new policy.

3. Editing hisecweb.inf using the Security Template Editor.

The Tool comes with a Microsoft Windows 2000 security template, hisecweb.inf. Hisecweb.inf also may be downloaded separately from the [Microsoft web site](#). The security template is edited using the SCE. The security template also may be applied independent of the Tool using the Security Configuration and Analysis (SCA) MMC snapin.

For more information on using and modifying Windows 2000 security templates using the SCE and the SCA, see the Windows 2000 Server online help, *sub voce* “Using Security Templates” and “Security Configuration and Analysis.” See also, [Security Configuration Toolset](#) and [Step-by-Step Guide to Using the Security Configuration Tool Set](#) on the Microsoft [Windows 2000](#) web site.

The SCE permits you to manage local and account security account, restricted groups, registry, file and system service policies using Microsoft Windows 2000 security

templates¹. In the following paragraphs we will briefly examine the security policies that the Tool sets using the default version of hisecweb.inf changes. Equally as importantly, we will note some of the things that the default hisecweb.inf template does not do.

3.1. Importing hisecweb.inf into the SCE.

Before you can edit hisecweb.inf, you need to import the file into the SCE. The [Secure Internet Information Services 5 Checklist](#) explains how to this. To edit hisecweb.inf, copy the file to your %windir%\security\templates directory on your local computer. Open the SCE and locate the hisecweb.inf template. [Figure 8](#) shows the open SCE with the hisecweb template highlighted.

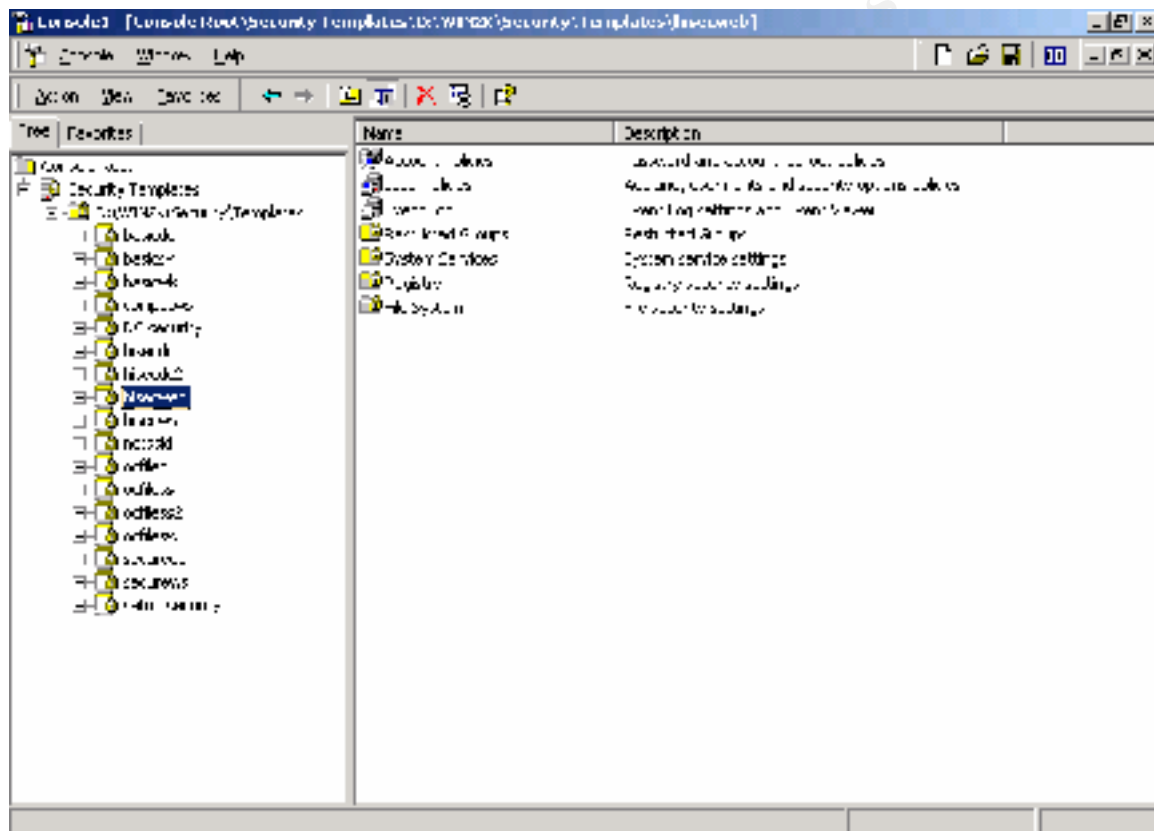


Figure 8. Locating the hisecweb security template in the SCE.

3.2. Account Policies.

Account policies are divided into password policies, account lockout policies and kerberos policies.

Hisecweb's account policies are identical to the policies recommended by the hisecdc and hisecws templates. Hisecweb enforces a password history of 24 passwords, a maximum password age of 42 days and a minimum password age of 2 days. Passwords are required

¹ The [Security Configuration Toolset](#) also mentions managing system store and Active Directory security policies using the SCE, however, this functionality does not appear to have made it into the final release.

to be 8 characters long and password complexity requirements are enforced. Hisecweb disables storage of passwords using reversible encryption. Hisecweb sets an account lockout threshold of 5 invalid logins and a lockout duration of 30 minutes. Once locked out an account will remain disabled until an administrator re-enables the account. Hisecweb does not establish a kerberos policy.

3.2. Local Policies.

Local policies are divided into an audit policy, a user rights assignment policy and a security options policy.

3.2.1. Audit Policies.

Hisecweb's audit policies are identical to the policies recommended by the hisecdc and hisecws templates with the following exceptions: Whereas the hisecdc and hisecws templates require auditing for both successful and failed object access, hisecweb requires auditing only for *failed* object access. This is a sensible change since auditing successful object access will generate an inordinate number of events in the security log thereby limiting the security log's utility. Also, the hisecweb template does not require auditing of Active Directory object access in contrast to the hisecdc template.

It is not generally recommended that you use a domain controller as a web server. If you do use your domain controller as a web server (perhaps on your corporate intranet), then you will want to enable auditing of failed directory object access.

The hisecweb template requires auditing for both successful and failed account logon events, account management, logon events, policy changes, privilege use and system events.

The hisec web template does not require auditing for process tracking.

3.2.2. User Rights Assignment.

The default access control settings for Microsoft Windows 2000 servers and workstations are described in the [Default Access Control Settings in Windows 2000](#) whitepaper. Workstation and server default settings differ in only one respect: On servers, Users are not granted the right to shutdown the system. The default user rights are designed to maintain backwards compatibility with existing applications and Microsoft operating systems. Thus, the default settings allow the Everyone group the right to access the computer from the network. This includes null session users. However, IIS does not require null session access. IIS maps anonymous users to the IUSR_computername account. This means that anonymous users will be Guests if IIS is installed on a server and Domain Users if IIS is installed on a domain controller. (This is one reason why IIS should not be installed on a domain controller.)

The hisecweb template properly restricts network access to authenticated users, which includes anonymous users. The template leaves the other default user rights assignment settings unchanged, however.

The problem with the default user rights assignment is that Authenticated Users are included within the definition of Users. This means that every right assigned to a *known* user is also assigned *ipso facto* to an *anonymous* user. There is no convenient way to assign a right to a User without also assigning the same right to an anonymous user. While this problem is more acute when configuring file and registry permissions, its implications need to be studied with respect to user rights assignment as well.

The default access permissions are quite generous in their assignment of rights to Power Users, also to maintain backward compatibility. Depending upon your company's user rights policy, you may want to consider further restricting the rights of Power Users.

3.2.3. Security Options.

The Default Security Options similarly are designed for backward compatibility with existing Microsoft operating systems. Most notably, the default installation of Microsoft Windows 2000 emulates NT 4.0 by leaving null session (anonymous²) users unrestricted, by sending both LM and NTLM response and by not requiring a strong session key. The default installation does enable many of the features introduced with Microsoft Windows NT 4.0 Service Pack 4 and later service packs. These features include enabling digital signing of client (but not server) communication and enabling digital signing and encryption of secure channel data. The default installation does not require digital signing of client communication or signing or encryption of secure channel data, however.

By contrast, the hisecweb template restricts null session access to what is explicitly permitted access. Digital signing of client *and* server communication is enabled and required. Use of the Backup and Restore privileges is audited. The LAN Manager authentication level is set to send only NTLMv2 and to refuse both LM and NTLM. Both digital signing and encryption of secure channel data are enabled and required. A strong Windows 2000 session key is required. The pagefile is cleared when the server shuts down. The recovery console is disabled. Device drivers are required to be signed.

Note that the hisecweb template defines a rudimentary logon banner. The banner reads: "ATTENTION: This is a private computer system. <add your own text>." You will probably want to "add your own text."

The hisecweb template does not rename the Administrator or Guest accounts. Obviously, it would not aid security much if everyone renamed these accounts to the same name. You will probably want to define these policies, however.

The hisecweb template disables eight-dot-three file creation.

² Note that "anonymous" users when used within the context of Microsoft Networking does not have the same meaning as "anonymous" users when used within the context of IIS.

The hisecweb template permits silent unsigned non-driver installation. You may want to modify this setting. However, be advised that you will not be able to do an unattended installation of Microsoft Windows 2000 Service Pack 1 if you do.

3.3. Eventlog.

The hisecweb template sets the size of the security log to 10240 kilobytes. The size of the application and system logs is not defined. The template restricts guest access to the application, security and system logs. The template does not define how long the logs are to be retained and it does not define the retention method for the application and system logs.

Note that the hisecweb template allows events in the security log to be overwritten “as needed.” Perhaps this is under the assumption that the large size of the security log will be accompanied with frequent backups so that security events never get overwritten. However, this setting will conflict with the security policies of many companies.

The hisecweb template does not require the system to shut down when the security audit becomes full.

Windows 2000 permits custom event logs. Needless to say, the template does not attempt to configure these logs.

3.4. Restricted Groups.

With Microsoft Windows NT 4.0, users frequently had to be added to the Power Users (or other) group to perform some momentary task. Often, system administrators would forget to remove the users after the task was completed. This meant that the Power Users (or other) group tended to grow to an inordinate size. Restricted Groups is a new feature that is intended to solve this problem.

According to the online documentation (*sub voce* “Restricted Groups”), Administrators, Power Users, Print Operators, Server Operators, and Domain Admins are automatically enrolled into Restricted Group membership. The hisecweb template adds Power Users. At first, this might appear redundant until you notice that the template does not assign any members to the Power Users Group. This means that the Power Users group will be emptied.

If you want anyone to remain a Power User group, you need to expressly add their user ids to the Power Users group in the template or they will be removed. Also note that the template does not make the Power Users group a member of any other group. Microsoft Windows 2000 also will remove the Restricted Group from membership in any other group unless that group is included in the definition of the restricted group. If you want the Power Users group to remain a member of any other group, you need to add that group to the definition of the Power Users group in the template.

3.5. System Services.

The default installation of Microsoft Windows 2000 includes many system services that are not required to operate a web server. The hisecweb template disables the following system services:

- Alerter Service;
- Clipbook Service;
- Computer Browser;
- DHCP Client;
- Fax Service;
- Internet Connection Sharing Service;
- Irmon Service;
- Messenger Service;
- Netmeeting Remote Desktop Service;
- Print Spooler;
- Remote Access Auto Connection Manager;
- Remote Access Connection Manager;
- Remote Registry Service;
- Task Scheduler;
- Telephony; and,
- Terminal Services.

Note that the Tool will alternately enable or disable the FTP, SMTP, NNTP and Telnet system services, depending on the information that you supply on the [IIS template configuration form](#). The hisecweb template does not configure these system services.

Note also that the hisecweb template does not disable the Server Service. IIS does not require the Server Service. However, the Server Service is required to remotely administer IIS using the Internet Information Services MMC snapin.

Depending on your configuration, you also may wish to disable the Network DDE and Network DDE DSDM Service, the Network Monitor Agent, Simple TCP/IP Services, the TCP/IP Netbios Helper Service and the NWLink Netbios Services.

3.6. Registry.

The hisecweb template configures a large number of registry keys. Unfortunately, these keys do not appear in the SCE because they are included under the “Registry Values” section rather than under the “Registry Keys” section. To obtain a full listing of the registry keys set by the hisecweb template, open the template into notepad.

The template configures a number of AFD ([MinimumDynamicBacklog](#), [EnableDynamicBacklog](#), and [DynamicBacklogGrowthDelta](#)) and TCP/IP ([TcpMaxDataRetransmissions](#), [TcpMaxConnectResponseRetransmissions](#), [DisableIPSourceRouting](#), [KeepAliveTime](#), [EnablePMTUDiscovery](#), [EnableDeadGWDetect](#), [SynAttackProtect](#) and [EnableICMPRedirect](#)) and NetBT

([NoNameReleaseOnDemand](#)) parameters. These changes are designed to thwart SYN and other denial of service attacks and to avoid fragmentation, ip spoofing and other malicious activities. For additional information on the significance of the tcp/ip and NBT registry values, see *TCP/IP & NBT Configuration Parameters for Windows NT*, KB [Q120642](#). See also, [Stevens, TCP/IP Illustrated. Volume 1. The Protocols](#) and Bisailon & Werner, [TCP/IP With Windows NT Illustrated](#).

The template disables hidden administrative shares. KB [Q245117](#). The template also enables security filters³. This activates the IPSec policy created by the Tool.

Note that the template disables web printing⁴. This would seem to be inconsistent with the [IIS template configuration form](#) that enables web printing in IIS if you select that option.

Note also that the template leaves the default security in place on the registry. It is not clear whether these default settings are adequate and further study is needed concerning this matter.

3.7. File System.

The hisecweb template does not change the default NTFS file permissions. This is a serious shortcoming of the Tool. [As has already been noted](#), the default rights and permissions are designed primarily to ensure backwards compatibility with existing Microsoft operating systems. This grants liberal access to the Everyone group to emulate null session users. IIS anonymous users do not require null session access. On the other hand, you would like to restrict anonymous Internet users to only those file and registry resources that they need. Currently, there is not convenient way to do this. Further study is needed as to what the appropriate NTFS permissions are for a web server.

4. Applying the Security Template to the Local IIS 5.0 Server.

Once you have edited hisecweb.inf to correspond to your company's security policy, you are ready to apply the IIS security template. You apply the IIS security policies by running a command script (IISConfig.cmd) that is located in the [Engine](#) subdirectory. The command script invokes cscript.exe to run a Jscript (IISConfig.js). The Jscript checks to see that you are logged on as an administrator and then iterates through the [IISTemplate](#) file that you created under [section 2](#), above. The script enables each Internet service that you selected (FTP, SMTP, NNTP, Telnet) and adds the appropriate ports to it port map. The script applies the security policies defined in hisecweb.inf by running secedit.exe. The script then configures the Script Map of the Default Web Site. Finally, the script creates an IPSec policy named "SecureWeb" by running ipsecpol.exe. As has already been noted, the default is to drop all traffic except for tcp traffic over port 80.

³ The parameter "EnableSecurityFilters" at HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameter is documented on the July MSDN CD *sub voce* "EnableSecurityFilters."

⁴ The parameter "DisableWebPrinting" at HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Printers is documented on the July MSDN CD. The value corresponds to the Administrative Template policy "Computer Configuration\Administrative Templates\Printers."

The IPSec policy also permits other ports as are required for the Internet or administrative services that you selected under [section 2](#), above.

The first time that I ran IISConfig.cmd, it created the SecureWeb IPSec policy and the policy was *assigned*, *i.e.* active. When I scanned using nmapNT (available from <http://www.eEye.com>) only port 80 was visible. However, I was able to see many ports open on my domain controller when scanning *from* my computer⁵. This suggests that the Tool is only setting an *ingress* filter. Egress filtering is also needed.

I was not able to replace the IPSec policy created during the first run of IISConfig, so I deleted the SecureWeb policy. Unfortunately, I have not been able to recreate the SecureWeb policy during subsequent runs of the command script. The Tool is still a little rough and will require a good deal of debugging before it will be ready for public consumption.

Nota Bene: Before you apply the template, remember to copy hisecweb.inf back into the [Engine](#). By default, the Tool will look for this template in the [Engine](#) subdirectory. You can specify a different path for the hisecweb.inf template from the command line. However, if you forget, the results may not be what you expect.

5. Conclusion.

The Internet Information Server Security Configuration Tool is an important step forward in the process of automating the configuration of IIS web server security. The Tool is still a little rough at the moment and does not always provide consistent results. The Tool does provide considerable insight into Microsoft's current thinking on web server security.

The Tool needs to be more thoroughly debugged. The Tool needs to be enhanced to adapt to common web scenarios, as Microsoft has already noted. In addition, registry and file system security needs to be addressed. The Tool needs to do more checking to make sure that IIS configuration is consistent with and implements the security and IPSec policies established by the Tool.

It should be noted that the Tool does not address one of the most important issues relating to web security, *i.e.* web application security. Operating system security is merely a prolegomenon to IIS security. IIS will never be more secure than the applications that run on it. For more information on building secure Internet applications on IIS, see Michael Howard, [Designing Secure Web-Based Applications for Microsoft Windows 2000](#).

6. References.

Architectural Design: A Scalable, Highly Available Business Object Architecture. URL:

⁵ I had hoped to repeat these scans so that they could be included in this article. However, I was unable to do so because the Tool is no longer functioning properly on this computer.

Bisaillon, Teresa and Brad Werner. *TCP/IP With Windows NT Illustrated*. New York: McGraw-Hill, 1998.

Brill, Jeffrey. *Windows 2000 Template Security Implications*. URL:
<http://www.sans.org/infosecFAQ/template.htm>.

Brown, Keith, *Web Security: Putting a Secure Front End on Your Com+ Distributed Applications*. URL:
<http://msdn.microsoft.com/msdnmag/issues/0600/websecure/websecure.asp>.

_____, *Web Security: Part 2: Introducing the Web Application Manager, Client Authentication Options, and Process Isolation*. URL:
<http://msdn.microsoft.com/msdnmag/issues/0700/websecure2/websecure2.asp>.

Cryptography and PKI Basics. URL:
<http://www.microsoft.com/windows2000/library/planning/security/pki.asp>.

Default Access Control Settings in Windows 2000. URL:
<http://www.microsoft.com/technet/win2000/win2ksrv/technote/secdefs.asp>.

Deploying Windows 2000 with IIS 5.0 for Dot Coms: Best Practices. URL:
<http://www.microsoft.com/technet/iis/iisdcom.asp>.

Fossen, Jason. *Internet Information Server* (July 5-10, 2000). The SANS Institute GIAC Training, 2000.

Howard, Michael, *Secure Internet Information Services Checklist*. URL:
<http://www.microsoft.com/technet/security/iis5ck.asp>.

_____. *Designing Secure Web-Based Applications for Microsoft Windows 2000*. Redmond, WA: Microsoft Press, 2000.

KB Q142641. URL: <http://support.microsoft.com/support/kb/articles/Q142/6/41.asp>.

KB Q165346. URL: <http://support.microsoft.com/support/kb/articles/Q165/3/46.asp>.

KB Q234905. URL: <http://support.microsoft.com/support/kb/articles/Q234/9/05.asp>.

Internet Information Services 5.0 Technical Overview. URL:
<http://www.microsoft.com/windows2000/library/howitworks/iis/iis5techoverview.asp>.

Lewis, Jason, *How to apply security policy to an Organizational Unit*. URL:
<http://www.jasonlewis.net/howto/secpolOU.asp>.

Microsoft Security Bulletin MS00-044. URL:
<http://www.microsoft.com/technet/security/bulletin/ms00-044.asp>.

Microsoft Windows 2000 Public Key Infrastructure. URL:
<http://www.microsoft.com/windows2000/library/howitworks/security/cryptpki.asp>.

Securing Windows 2000 Network Resources. Scenario Guide. URL:
<http://www.microsoft.com/windows2000/library/incremental/securenetworkresources.asp>.

Security Configuration Toolset. URL:
<http://www.microsoft.com/windows2000/library/howitworks/security/sctoolset.asp>.

Server-Side Includes Reference. URL:
<http://msdn.microsoft.com/library/psdk/iisref/serv9i5h.htm>.

Step-by-Step Guide to Using the Security Configuration Tool Set. URL:
<http://www.microsoft.com/windows2000/library/planning/security/secconfsteps.asp>.

Stevens, W. Richard. *TCP/IP Illustrated*. Volume 1. *The Protocols*. Reading, MA: Addison-Wesely, 1994.

TCP/IP & NBT Configuration Parameters for Windows NT, KB Q120642. URL:
<http://support.microsoft.com/support/kb/articles/Q120/6/42.asp>.

The Art and Science of Web Server Tuning with Internet Information Services 5.0. URL:
<http://www.microsoft.com/windows2000/library/operations/web/tuning.asp>.

Understanding Active Server Pages. URL:
<http://msdn.microsoft.com/library/psdk/iisref/iowaaspw.htm>.

© SANS Institute 2000 - 2002. Author retains full rights.