Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

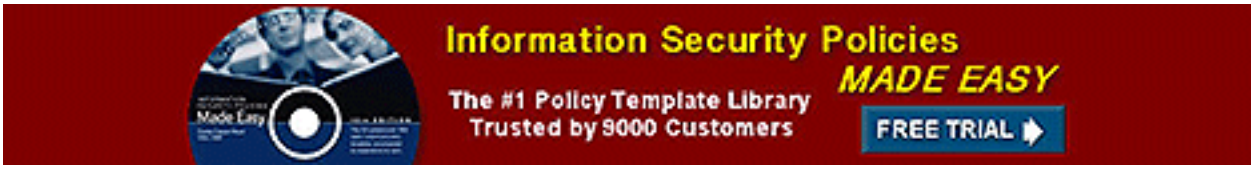
This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

What Does It Take to Harden an IIS Web Server?

In order to secure a Windows system, you need to have a good understanding and knowledge of the underlying system as well as the latest security fixes. Systems can never be 100% safe from an intruder but systems administrators can minimize the system exposure by building an extra wall to deter the would be attackers. This can be achieved by applying up to date security patches, hardening the OS, hardening IIS 5.0 and system(s) scanning using Nessus. The purpose of this document is to shed some light on how to make it h...

Copyright SANS Institute
Author Retains Full Rights

AD



SANS Security Essentials Practical Assignment

What does it take to harden an IIS Web server?

Author: Boris Napernikov
Date: Tuesday, February 19, 2002
Version: 1.3

Table of Contents

Abstract **2**
Introduction **2**
General Information on the tools **3**
Windows 2000 & IIS Installation Tips **3**
SECURING/HARDENING WINDOWS 2000 ..... **4**
Applying Patches 5
Security Configuration 6
Local security options 7
SECURING/HARDENING IIS 5.0 ..... **11**
Enable Logging 17
System Scanning **17**
Nessus 17
Comments **19**
References **20**

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Abstract

In order to secure a Windows system, you need to have a good understanding and knowledge of the underlying system as well as the latest security fixes. Systems can never be 100% safe from an intruder but systems administrators can minimize the system exposure by building an extra wall to deter the would be attackers. This can be achieved by applying up to date security patches, hardening the OS, hardening IIS 5.0 and system(s) scanning using Nessus.

The purpose of this document is to shed some light on how to make it harder for an intruder to compromise the system. We'll be going through securing a Windows 2000 server running IIS 5.0 and some of the tools that we can use to scan system(s) before putting it into production.

Introduction

Most people would agree that the Internet is not the safest place to be, however with the increasing demands on businesses to maintain an online presence as well as use online/internet technologies to provide remote access to corporate information, companies have to make sure that their systems and the information within is not vulnerable to attackers. A high level of system security can only be achieved through a combination of policy, software and hardware. Systems administrators should harden/secure system(s) not only to protect corporate data but also help prevent spreading of viruses, worms, participations in DDoS (Distributed Denial of Service) attacks etc. Viruses and worms are so advanced these days that once a system becomes a victim of it, the system will start to spread the virus/worm to other systems internally (LAN/WAN) and externally (Internet) causing network congestions and outages. A good example of a worm that could potentially cause these types of attacks is the Nimda worm. Nimda is an Internet worm that spreads via a number of different methods including exploiting several known vulnerabilities in Internet Explorer and IIS systems. It also works as a virus, which infects executable files (.exe) as well as files with extensions html, htm, and asp. This worm can infect a system in the following ways;

- Via a html e-mail with a specifically constructed MIME header
- By visiting a Web site hosted on an infected system
- Via open network shares
- Via unpatched IIS system (both IIS4.0 and IIS5.0)

There is vulnerability with 'Incorrect MIME Header' in Microsoft Internet Explorer 5.01 and 5.5, which may launch the attached program, executing the Nimda code. The worm may also exploit security holes in systems running Microsoft IIS in the following ways;

- Microsoft IIS 4.0/5.0 File permission canonicalization vulnerability
- Microsoft IIS/PWS (Personal Web Server) escaped character decoding command execution vulnerability
- Microsoft IIS/PWS extended Unicode directory traversal vulnerability

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

(CA (Computer Associates), http://www3.ca.com/Virus/Virus.asp?ID=10397)

General Information on the tools

Some of the utilities/tools that we'll be using in this document are free to download to use; (Note that there are many other utilities/tools that are available for commercial usage that we will not be covering in this document)

- **HFNETCHK** – You can use the Hfnetchk tool to assess patch status for computers that are running Windows NT 4.0, Windows 2000, and Windows XP, as well as hotfixes for Internet Information Server 4.0 (IIS), Internet Information Services 5.0 (IIS), SQL Server 7.0, SQL Server 2000 (including Microsoft Data Engine [MSDE]), and Internet Explorer 5.01 or later. (Microsoft KB article Q303215, http://support.microsoft.com/directory/article.asp?ID=KB;EN-US;q303215)
- **IISLOCKD** – IIS Lockdown works by turning off unnecessary features, thus reducing attack surface available to attackers. To provide multiple layers of protection against attackers, URLscan, with customized templates for each supported server role, is integrated into the IIS Lockdown Wizard.
  To keep the server completely secure, however, all hotfixes are required before and after applying IIS Lockdown to stay protected against known security vulnerabilities. (Microsoft, http://www.microsoft.com/Downloads/Release.asp?ReleaseID=33961)
- **NESSUS** – A security software scanner, which will audit systems and determine whether bad guys (aka 'Crackers') may break into it, or misuse it in some way. (Nessus, http://www.nessus.org/intro.html)
- **STUNNEL** – Stunnel is a program that allows you to encrypt arbitrary TCP connections inside SSL (Secure Sockets Layer) available on both Unix and Windows. This utility will only be used if SSL is enabled on the IIS 5.0 Server. (Stunnel, http://www.stunnel.org)

Windows 2000 & IIS Installation Tips

In order for a system to be secure, the system must be installed with the minimal options required for its functionality. Take for example the installation of Windows 2000; the default settings will install IIS (Internet Information Service) with the options of SMTP (Simple Mail Transport Protocol), FTP (File Transport Protocol), WWW (World Wide Web) and FrontPage extension service. If the only requirement for this system is to be a WWW server, then there is absolutely NO need to install any other options. Installing the other options will only make your system more vulnerable to the hackers/crackers that use the weaknesses in these programs to access your system. (You can find many vulnerabilities and exposures for these services at http://cve.mitre.org/cve/ or http://www.securityfocus.com/bid). Try it out, go to http://cve.mitre.org/cve/ and do a

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

search by Keyword(s) and type in FrontPage. I can tell you now that you'll be very surprised.

To keep the options to a minimal, during the installation uncheck IIS (Internet Information Service 5.0) and go into the details section and select only WWW (World Wide Web). You'll notice that by selecting WWW (World Wide Web), only Common Files and Internet Information Services Snap-In gets checked automatically, this is all that you will need for WWW to run.
One other thing to take note of is to make sure that the file system is NTFS. If the file system is not NTFS, you can use the CONVERT.exe utility to change the file system from FAT to NTFS. The reason for this is because Windows NT only manages security on NTFS file system. Take note that, after using the convert.exe utility, it will set the ACLs (Access Control List) for the converted drive(s) to Everyone:Full Control. Make sure that you use the fixacls.exe utility from the resource kit to reset them to a reasonable value.

SECURING/HARDENING WINDOWS 2000

Once the operating system has been installed, remove the network cable from its port, log onto the system as local administrator and stop the World Wide Web service. Once this service is stopped, reconnect the network cable back into the network socket. (This will reduce the chances of viruses like Nimda/Code Red infecting your system by vulnerability within IIS 4.0 / 5.0). When the system gets a network connection, you'll need to download the following;

- Windows 2000 SP2, this provides the latest updates to the Windows 2000 operating systems. These updates are a collection of fixes for application compatibility, operating system reliability, security and setup. For example, it upgrades the system from 56-bit encryption to 128-bit encryption, which improves the security of local data and online transactions as well as shared content over networks or the Internet. (Download from: http://www.microsoft.com/Windows2000/downloads/servicepacks/sp2/download.asp)
- Windows 2000 security rollup package, this contains a cumulative rollup of security updates that have been offered since the release of Windows 2000 Service Pack 2. It includes things such as a patch for MIME Header Denial of Service Vulnerability. (Microsoft KB article Q311401, http://www.microsoft.com/windows2000/downloads/critical/q311401/default.asp)
- HFNETCHK, this is a tool which allows system administrators to assess a system or a group of systems for the absence of security patches via a command line. This tool can be used to assess patch status for system(s) that are running Windows NT 4.0, Windows 2000, Windows XP as well as hotfixes for IIS 4.0, IIS 5.0, SQL 7.0, SQL 2000 (including Microsoft Data Engine [MSDE]) and IE

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

5.01 or higher. (Microsoft KB article Q303215, http://support.microsoft.com/directory/article.asp?ID=KB;EN-US;q303215)

- IISLOCKD (IIS Lock Down), this provides a template, which works by turning off unnecessary features which reduces the attack areas available to hackers. It also provides an in depth defense or multi layers of protection against hackers by using URLscan via a customized template for each supported server role which is integrated into IISLOCKD Wizard. Note: all hotfixes are required to protect against known vulnerabilities. An example of the features is to remove or disable IIS services such as HTTP, FTP, SMTP and NNTP. (Microsoft, http://www.microsoft.com/Downloads/Release.asp?ReleaseID=33961)

Applying Patches

Once you've downloaded all of the above, disconnect your machine from the network again by unplugging the network cable and start installing the patches in the following sequence;

- Apply the Windows 2000 service pack 2 and reboot
- Apply SRP1 and reboot
- Extract HFNETCHK to C:\HFNETCHK
- Connect machine back onto network, ensure that system has Internet connectivity
- Run Windows Update by going to *Start-> Windows Update*
- Scan for updates and upgrade IE 5.x to IE.60, once installation is finish, reboot
- Run Windows Update again
- Scan for updates, this time select 'Critical Updates', reboot once install finishes (Critical updates contain security fixes, including fixes for IE 6.0 that's why upgrade IE first. Note: Microsoft goes through security test processes before they actually make it available to critical updates, which means that a new security patch may have a 3 weeks delay. As a result, it's best to subscribe to the Microsoft Security Notification Service, which provides notification of new vulnerability information and fixes for Microsoft products. Refer to. http://www.microsoft.com/technet/security/bulletin/notify.asp)
- Open a command prompt and go to the C:\HFNETCHK directory
- From the command prompt type 'Hfnetchk –v –z –s 1' (make sure that you have Internet access from the system that you're executing this command from) Here is what it should look like; (Performed on a Windows XP system)

C:\hfnetchk>hfnetchk –v –z –s 1
Microsoft Network Security Hotfix Checker, 3.32
Copyright (C) Shavlik Technologies, 2001-2002
Developed for Microsoft by Shavlik Technologies, LLC
info@shavlik.com (www.shavlik.com)

Attempting to download the CAB from:
http://download.microsoft.com/download/xml/security/1.0/NT5/EN-US/mssecure.cab

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

File was successfully downloaded.

Attempting to load D:\hfnetchk\mssecure.xml.
Using XML data version = 1.0.1.174 Last modified on 12/20/2001.

Scanning HOSTNAME
….....
Done scanning HOSTNAME
HOSTNAME (10.10.22.25)

- *WINDOWS XP GOLD*

  Information
  All necessary hotfixes have been applied

- *INTERNET EXPLORER 6 GOLD*

  Information
  All necessary hotfixes have been applied

When the system returns with 'All necessary hotfixes have been applied' this completes the patch update process. If it returns with a different message with a QXXXXXX number, go to the Microsoft Knowledge Base site and search for further information basing your search on the QXXXXXX number.
http://support.microsoft.com/default.aspx?scid=fh;rid;kbinfo

Security Configuration

To further secure the system and enable auditing, follow the following steps:

Rename the Administrators Account
To eliminate the chances of an attacker who may try to 'brute force' the Administrators account, rename the account so that it is harder for hacker(s) to find out the admin account.

Strong Administrators Password
Windows 2000 allows passwords of up to 14 characters. For maximum protection, make sure the Administrators account's password is at least 9 character long and that it includes punctuation marks, and contains non-printing ASCII characters (generated by using the Alt key and 3 digit key codes on the numeric keypad) within the first 7 characters.

Ensure that the Guest Account is disabled
By default, the Guest account is disabled on Windows 2000 systems. Double-check and make sure that it is disabled.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Unbind/Remove unnecessary protocols

If you have any other protocols installed on the system(s) besides TCP/IP, like IPX/SPX or NetBEUI etc, consider either removing them or unbinding them from the network interface that will be connected to the outside (DMZ).

Disable NetBIOS over TCP/IP (Optional but highly recommended if NetBIOS is not required)

This prevents attackers from executing the NetBIOS Adapter Status command against the system(s), the NetBIOS Adapter Status command reveals the name of the most current user logged on which could be used maliciously by an attacker. Important Note: Before disabling NetBIOS over TCP/IP, systems administrators need to ensure that disabling NetBIOS will not affect any other applications or management tools which are used to manage the system(s) remotely.

Local security options

Security Options

You can use the Windows 2000 local security policy editor to further secure the system. To open the Local Security policy console, click **Start**, click **Run** and type **Secpol.msc /s**. Click **OK**. Under Local Policies | Security Options, the following settings will be applied:

Additional restrictions for anonymous connections- set to 'No access without explicit anonymous permissions'

The LSA handles aspects of security administration on system(s), including access and permissions. System administrators should restrict anonymous user(s) so the amount of public information they can obtain about the LSA component of a Windows 2000 security subsystem is reduced. The restrictions can also be performed by, editing the following registry entry:

Hive	HKEY_LOCAL_MACHINE\SYSTEM
Key	CurrentControlSet\Control\LSA
Value Name	RestrictAnonymous
Type	REG_DWORD
Value	2

Clear virtual memory pagefile when system shuts down- set to 'Enable'

By clearing the paging file upon system shutdown will ensure that no unsecured data is contained in the paging file when the shutdown process is complete. This can also be performed by, editing the following registry entry:

Hive	HKEY_LOCAL_MACHINE\SYSTEM
Key	CurrentControlSet\Control\Session Manager\Memory Management

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Value Name	ClearPageFileAtShutdown
Type	REG_DWORD
Value	1

Do not display last user name in logon screen- set to 'Enable'

By default, the name of the last successfully logged on user will be displayed in the logon dialog box. This can also be performed by, editing the following registry entry:

Hive	HKEY_LOCAL_MACHINE\Software
Key	Microsoft\WindowsNT\CurrentVersion\winlogon
Value Name	DontDisplayLastUserName
Type	REG_DWORD
Value	1

LAN Manager Authentication Level- set to Send LM & NTLM – use NTLMv2 session security if negotiated.

Windows NT supports two variants of challenge/response authentication for network logons:

- LAN Manager (LM) challenge/response
- Windows NT challenge/response (also known as NTLM version 1 challenge/response)

The LM variant allows interoperability with the installed base of Windows 95 clients and servers. NTLM provides improved security for connections between Windows NT clients and servers. Windows NT also supports the NTLM session security mechanism that provides for message confidentiality (encryption) and integrity (signing).
Recent improvements in computer hardware and software algorithms have made these protocols vulnerable to attacks that try to obtain user passwords. In its ongoing effort to deliver more secure products to its customers, Microsoft has developed an enhancement, called NTLM version 2, which significantly improves both the authentication and session security mechanisms. NTLM 2 has been available for Windows NT 4.0 since Service Pack 4 (SP4) was released, and it is supported natively in Windows 2000. You can add NTLM 2 support to Windows 95 and Windows 98 by installing the Directory Services Client from the Windows 2000 CD-ROM.
(Microsoft, KB article Q239869)

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

User Rights Assignment

From the Local Security policy console, under Local Policies | User Rights Assignment, set the following: (only the important notes and changes made to the default are covered below)

Act as part of the operating system	*** Do NOT assign to any user ***
Create a token object	*** Do NOT assign to any user ***
Debug Programs	Remove Administrators (This is not auditable and should not be assigned to anyone)
Generate security audits	*** Do NOT assign to any user ***
Log on locally	Remove Guest, Users, Power Users, Backup Operators as desired
Replace a process level token	*** Do NOT assign to any user ***

Audit policy

Enabling auditing on a system is a very effective way of monitoring system activities including user logons, user account management etc. To enable auditing, from the Local Security policy console, under Local Policies | Audit Policy, set the following: (Note: its common practice to review the security event logs periodically to check for unusual frequency of these failures)

Policy	**Local Settings**
Audit account logon events	Success, Failure
Audit account management	Failure
Audit directory services access	No auditing
Audit logon events	Success, Failure
Audit object access	No auditing
Audit policy change	Failure
Audit privilege use	Failure
Audit process tracking	No auditing
Audit systems events	No auditing

By default Windows systems sets the event logs (Application, Security, System) to a size of 512KB, with the option of 'Over write events older then 7 days'. These settings can be changed from the Computer Management console. Click **Start**, click **Run**, and then type **compmgmt.msc /s** into the text box and click **OK**. Click the + sign to open Event Viewer. Right click on each of the event log (Application, Security, and System) and select properties. From the properties page, log size settings as well as what the system should do once the log reaches the maximum size that is allocated in the Maximum Log size field.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Account Password/Lockout Policy

It is imperative to have blank passwords disabled on any system(s) that will be used in production. Disabling blank passwords and setting up a strong account policy will be covered in this section. From the Local Security policy console, under Account Policy, set the following:

Password Policy

Policy	**Local Settings**
Enforce password history	6
Maximum password age	30
Minimum password age	1
Minimum password length	8

Account Lockout Policy

Policy	**Local Settings**
Account lockout duration	30 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	30 minutes

Restrict attacker's ability to plant Trojan programs

Trojan programs can take advantage of the system's Run Utility (registry) if it is not restricted. Trojan programs, when run might try to create backdoors like NetBUS or damage the system by running format upon reboot etc. Restriction can be applied to Run, RunOnce etc in the registry:

- Use the registry editor (regedt32.exe) to locate the following keys:

Hive	HKEY_LOCAL_MACHINE\SOFTWARE
Key	Microsoft\Windows\CurrentVersion
Values	Run, RunOnce, Uninstall (if present), AEDebug and all their subkeys

- Select each of the subkeys, from the Security menu select Permissions
- For each of the subkeys selected, set the permissions for everyone and all untrusted users to a maximum of 'Read'

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

SECURING/HARDENING IIS 5.0

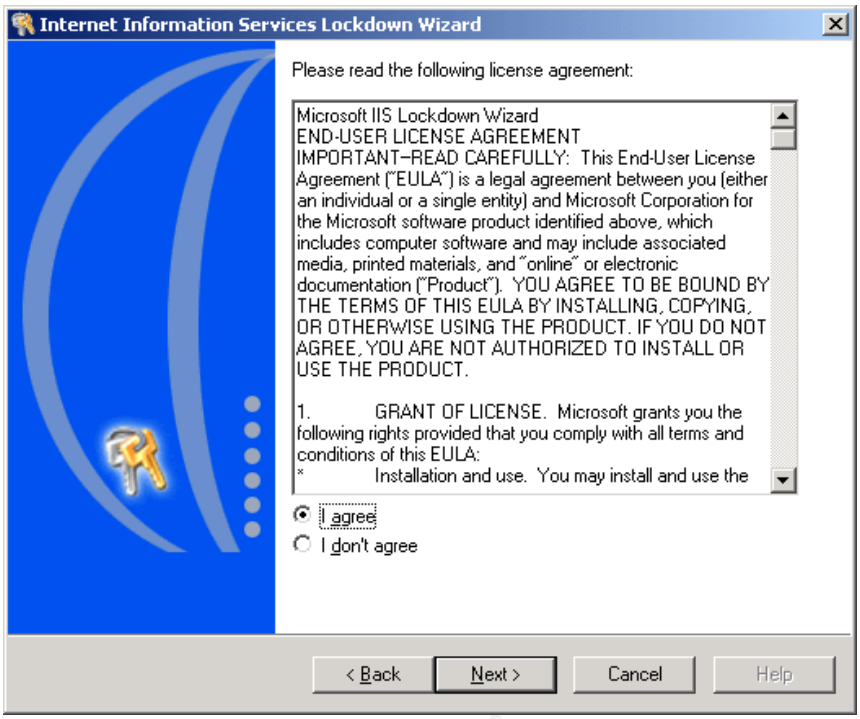
Microsoft has released a utility (IISLOCKD) that secures the IIS to a large extent. When run, this utility will disable and remove any unnecessary feature from IIS which might pose a security risk. Any changes made by using the IISLOCKD utility can be reverted by re-running it again.

The following is a step-by-step guide with snapshots, which will harden IIS 5.0.

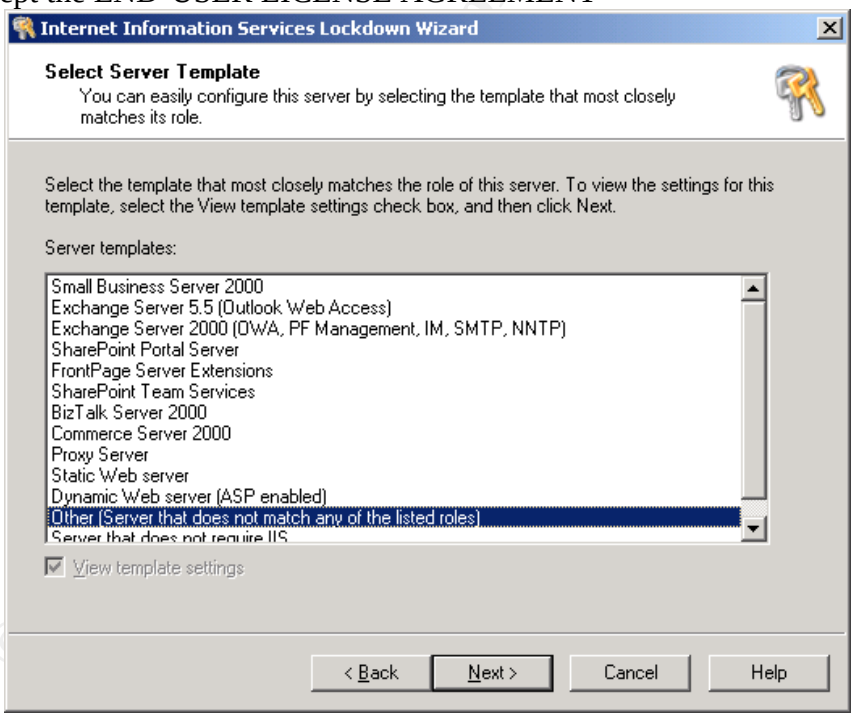
- Run IISLOCKD.exe that you've downloaded from the Microsoft Web site

- Click Next to continue

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

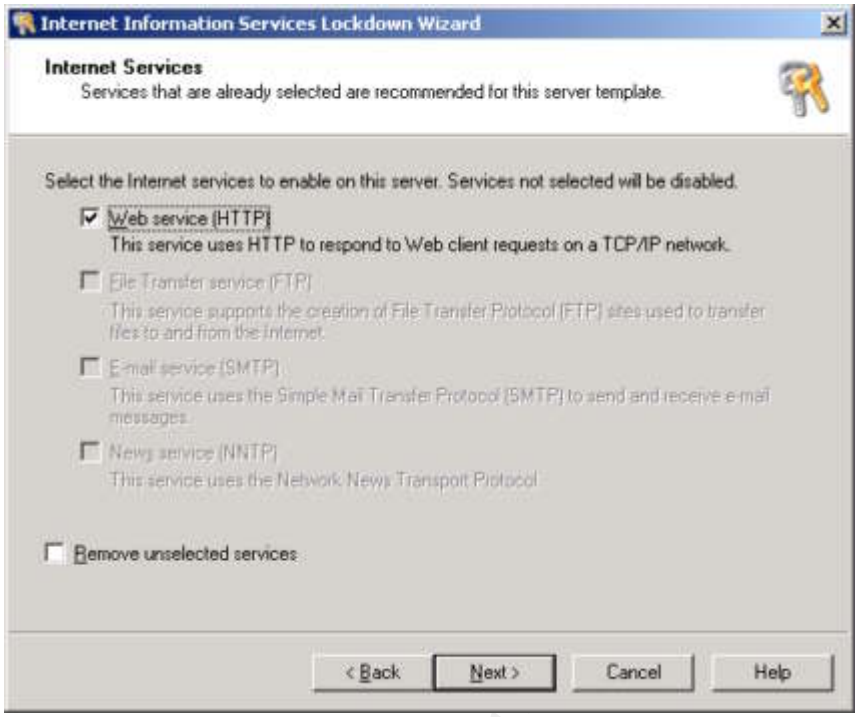


- Accept the END-USER LICENSE AGREEMENT

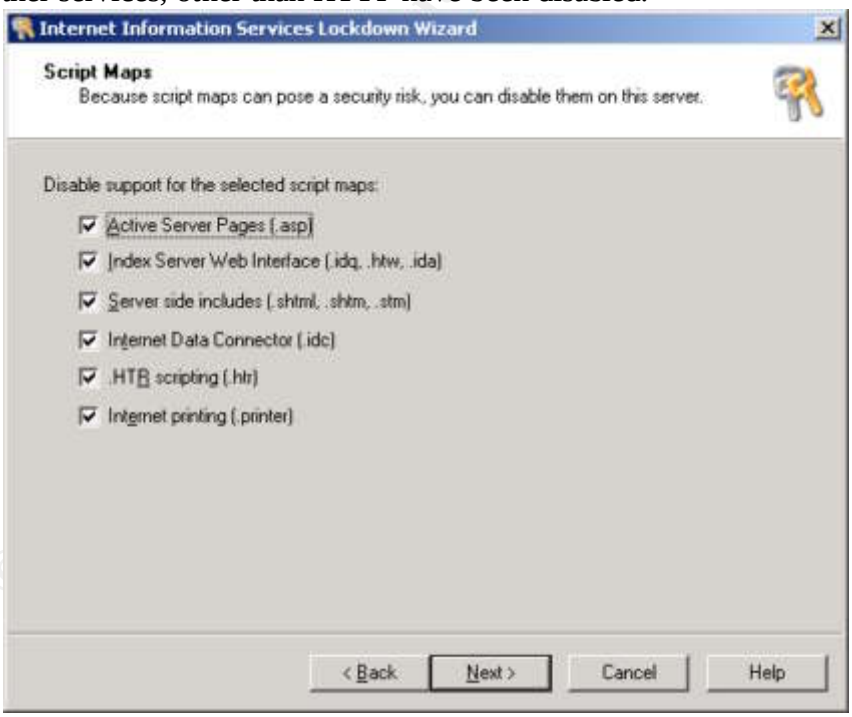


- Choose a template, which will best suit your requirements. Make sure that the check box ***View template settings*** is checked, this will allow you to see what the template is locking down and allow you to alter it if necessary. To totally customize this process, choose Other ***(Server that does not match any of the listed roles)***

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.



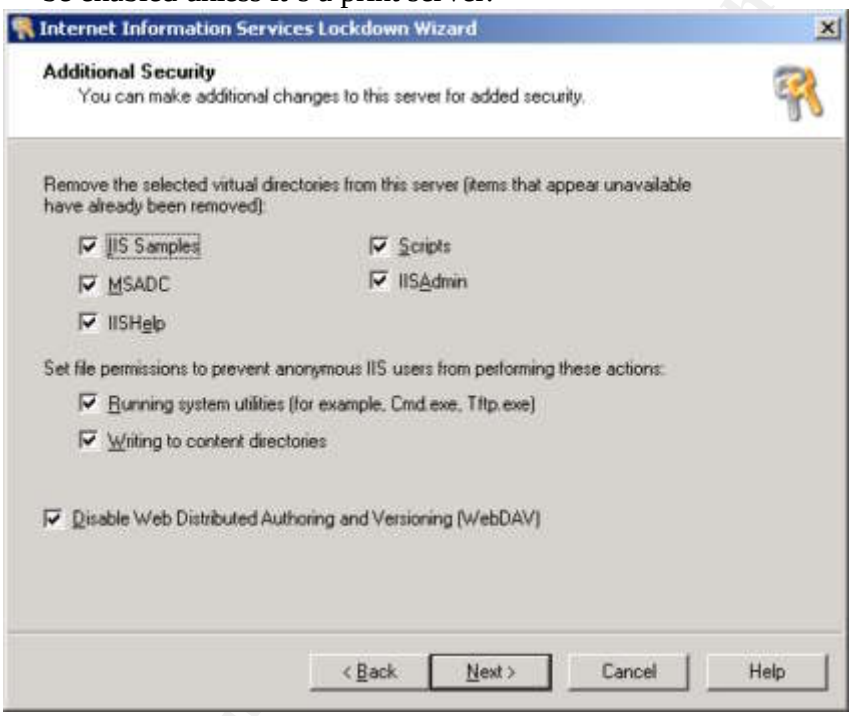
- Select only the services that you require, do NOT select any services that you do not require. In this example, since the system is to be setup as a Web server only, all other services, other than HTTP have been disabled.



- Unless there is a requirement for any of these script mappings by an application, it should be turned off.
    - Active Server Pages – If the Web server is going to host .asp extensions, then this should not be turned off.

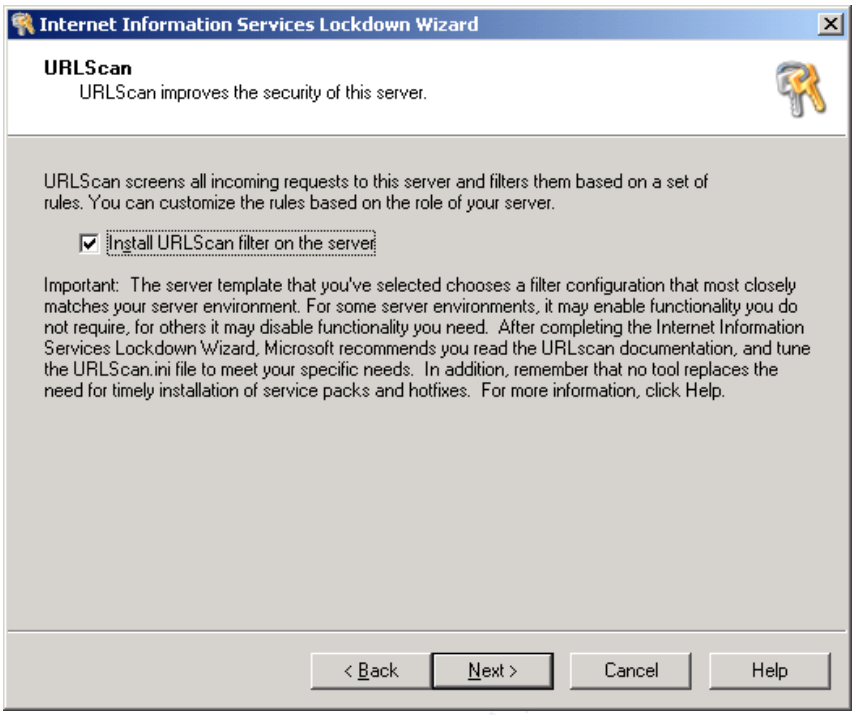
© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Index Server Web Interface – This component was the basis for the Code Red / Nimda exploit.
- Server Side Include – Server side include help to download data to clients automatically.
- Internet Data Connector – IDC is used for dynamic Web page updating. It is a legacy component and should not be necessary.
- .HRT – Used for Web based password resets. This feature should be turned off unless you have SSL and Authentication enabled.
- Internet Printing – Support for Internet printing protocol, this should not be enabled unless it's a print server.

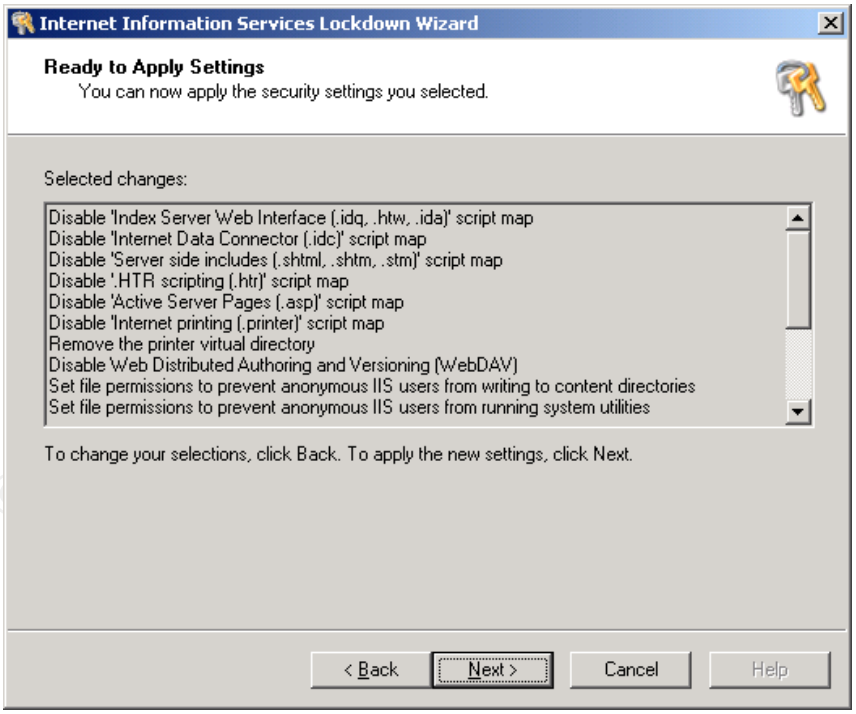


- Again, all these virtual directories should be removed unless there is a requirement to leave them on
  - IIS Samples – Sample IIS files, these are only samples, they definitely should be removed
  - Scripts – VB Scripts provided with Active Server Pages
  - MSADC – Used for Web based data access
  - IISAdmin – Used for Web Administration
  - IISHelp – Used for IIS Help (normally http://hostname/iishelp) this virtual directory should be removed
  - Set restrictive file permission for the Internet guest account, they should not have the ability to execute any commands
  - WebDAV is a set of extensions to the HTTP protocol which enables users to collaboratively edit and manage files on remote Web servers

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

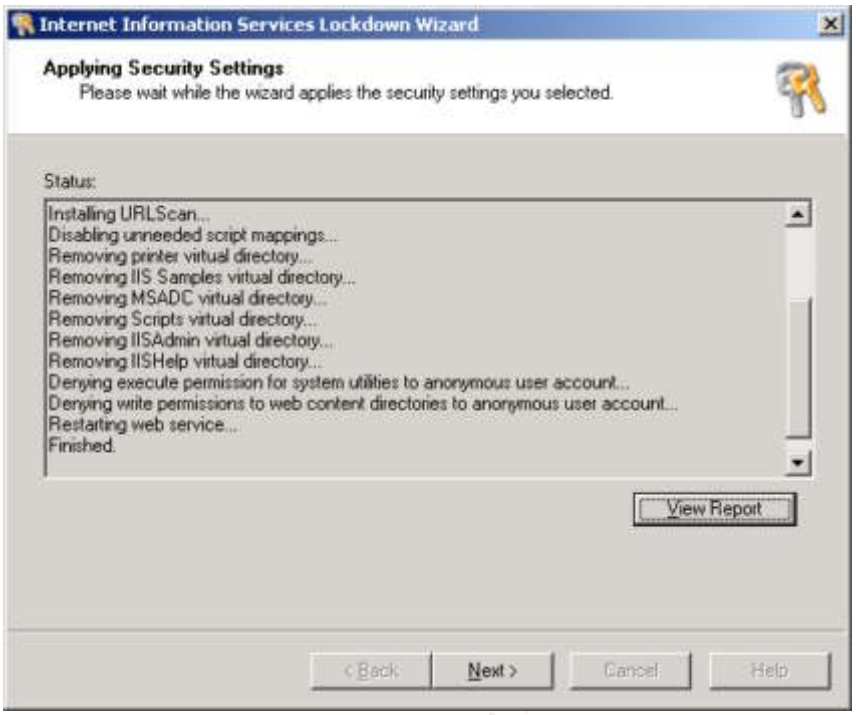


- The URLScan ISAPI filter screens inbound HTTP requests to the Web server, which can secure the Web server against a variety of known and unknown attacks. The filter uses rules to block requests that contain potential dangerous strings that could compromise a Web server. This feature adds another layer of security for Web servers



- This screen shot provides information about services being disabled, virtual directories being removed and file permissions being set on certain files/directories.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.



- This screen shot provides information on the installation of URLScan and script mappings being disabled.

- Click Finish to complete the Wizard

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Enable Logging

Logging is a must when you want to see if your server has been compromised. You should use W3C Extended Logging format by loading the IIS MMC tool | Right-click on the site | Properties | Web Site | Enable Logging (W3C Extended Log), then set the following properties;

- Client IP Address
- User Name
- Method
- URI Stem
- User Agent
- Server IP Address
- Server Port

Make sure you are not indexing confidential source code.

Last but least, make sure the ACLs on the IIS generated log files (%systemroot%\system32\LogFiles) are;

- Administrators (Full Control)
- System (Full Control)
- Everyone (RWC)

System Scanning

Nessus

This section will cover the use of Nessus for the purpose of scanning system(s) for known vulnerabilities and finding solutions according to the report generated by the scanner (Nessus).

> Nessus is made up of two parts: a server and a client. The server (nessusd) is actually in charge of the attacks, whereas the client is just a front-end designed to collect the results. As of today, there is only one version of the server which works on POSIX systems (Solaris, FreeBSD, GNU/Linux and others), and there are three clients: one which works with GTK (the Gimp ToolKit, another has been written in Java, and the last one works under Windows.
> *The server is not an option*. It performs the security checks.
> (Nessus, http://www.nessus.org/download.html)

Installing Nessus (this needs to be performed on a POSIX system)

- From one of the Nessus mirrored sites, download nessus-installer.sh (it's assumed, nessus-installer.sh is downloaded into the /home/downloads directory)
- Once the download is complete, open a terminal console and go to the /home/downloads directory

© SANS Institute 2002, Author retains full rights.

- Execute the shell script by typing in sh nessus-installer.sh (this performs the installation automatically)
- Once the installation is complete, download the latest plugins (ie. Each plugin represents a certain vulnerability, currently there are over 800 plugins) to /home/downloads/plugins from http://www.nessus.org/nasl/all.tar.gz (all.tar.gz file, this contains all the plugins up to date)
- Once the plugins download is complete, go to the /home/downloads/plugins directory using the terminal console
- Type in gunzip all.tar.gz to unzip
- Type in tar xvf all.tar to untar the plugins
- Copy all the .nasl file to the nessus plugin library located under /usr/local/lib/nessus/plugins

Starting Nessus Daemon

- To start the Nessus daemon, go to /usr/local/sbin and type in ./nessusd –D

Create a Login ID

- To create a login ID for nessus, go to /usr/local/sbin and type in ./nessus-adduser and go through the step by step process to create a login ID

Starting Nessus Client

- To start the Nessus client, go to /usr/local/bin and type in, ./nessus
- A GUI will pop up asking for a pass phrase (password)

Nessus setup

- Once pass phrase has been accepted, the "Nessus Setup" interface will pop up
- Click on the Login button to log onto the Nessus server (daemon)
- Click on the "Plugins" tab, click on the "Enable all" button, this will select all the plugins
- Click on the "Target selection" tab, and enter IP Address or the Host Name of the system that will be scanned in the "Target(s)" field

Stating scan

- Once all the setup is complete click on the "Start the scan" button, at the bottom of the "Nessus setup" GUI to start the scan.

Analyzing report

Upon completion of the scan, a report is generated by Nessus. In this report, Nessus provides a list of High, Medium and Low priority vulnerabilities. Systems administrators should address all the identified vulnerabilities that are likely to pose a risk to the system.

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Stunnel (If SSL is enabled on Web server)

SSL (Secured Socket Layer) security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection. (Netscape, http://www.netscape.com/security/techbriefs/ssl.html). Since Nessus does not support scanning SSL, Stunnel can be utilized to build like a SSL tunnel through a client system for Nessus to perform a secured scan.
"Stunnel is a program that allows you to encrypt arbitrary TCP connections inside SSL". (Stunnel, http://www.stunnel.org),

Utilizing Stunnel

- From a Windows client system download a Windows version of Stunnel (Stunnel-3.22.exe, libssl32.dll, libeay32.dll) from http://www.stunnel.org/download/binaries.html to C:\Stunnel
- Open a command prompt and go to C:\Stunnel
- At the C:\Stunnel command prompt, type in Stunnel-3.22.exe –c –d 80 -r hostname:443 to build a SSL tunnel between the client system and the Web server
- Nessus is now able to scan the SSL channel through the client machine to the Web server

Comments

Securing system(s) is not the complete fix, as there will always be an attacker who will find alternate areas to compromise. As a result, when considering security of a system you will need to determine all the possible threats, vulnerabilities and attacks. The number of incidents reported by CERT (Computer Emergency Response Team at Carnegie Mellon University) for the year 2000 was 21,756 and last year 2001 alone has gone over twice the amount to 52,658. (For further statistics, refer to: http://www.cert.org/stats/).

Thus, the most important advice to keep in mind as a systems administrator is to know about your system and having access to current news on security. There are many sites and mailing lists, which provide a systems administrator with up to date information on new exploits found. A good place to start is at http://www.securityfocus.com.

© SANS Institute 2002, Author retains full rights.

References

- Computer Associates Int'l – Information on Nimda virus
  http://www3.ca.com/Virus/Virus.asp?ID=10397

- Microsoft Corporations – Information on Windows 2000 Service Pack 2
  http://www.microsoft.com/windows2000/downloads/servicepacks/sp2/default.asp

- Microsoft Corporations – Information on Windows 2000 Security Rollup Package
  http://www.microsoft.com/windows2000/downloads/critical/q311401/default.asp

- Microsoft Corporations – Information on IISLOCKD
  http://www.microsoft.com/Downloads/Release.asp?ReleaseID=33961

- Microsoft Corporations – Information on HFNETCHK
  http://support.microsoft.com/directory/article.asp?ID=KB;EN-US;q303215

- Microsoft Corporations – Information on LM, NTLM and NTLMv2
  http://support.microsoft.com/default.aspx?scid=kb;EN-US;q239869

- Nessus – Information on Nessus software security scanner
  http://www.nessus.org/intro.html & http://www.nessus.org/download.html

- Stunnel – Information on Stunnel http://www.stunnel.org

- Common Vulnerabilities and Exposures – Information on vulnerabilities and exposures http://cve.mitre.org/cve/

- SecurityFocus – Information on vulnerabilities and exposures
  http://www.securityfocus.com/bid

- Netscape – Information on SSL http://www.netscape.com/security/techbriefs/ssl.html

- CERT (Computer Emergency Response Team at Carnegie Mellon University) – Information on incident statistics http://www.cert.org/stats/

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: February 7th, 2016

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Secure Japan 2016	Tokyo, JP	Feb 15, 2016 - Feb 20, 2016	Live Event
SANS Northern Virginia - McLean 2016	McLean, VAUS	Feb 15, 2016 - Feb 20, 2016	Live Event
SANS Munich Winter 2016	Munich, DE	Feb 15, 2016 - Feb 20, 2016	Live Event
ICS Security Summit & Training - Orlando	Orlando, FLUS	Feb 16, 2016 - Feb 23, 2016	Live Event
SANS Secure India 2016	Bangalore, IN	Feb 22, 2016 - Mar 05, 2016	Live Event
SANS Southern California - Anaheim 2016	Anaheim, CAUS	Feb 22, 2016 - Feb 27, 2016	Live Event
RSA Conference 2016	San Francisco, CAUS	Feb 28, 2016 - Feb 29, 2016	Live Event
SANS Philadelphia 2016	Philadelphia, PAUS	Feb 29, 2016 - Mar 05, 2016	Live Event
SANS London Spring 2016	London, GB	Feb 29, 2016 - Mar 05, 2016	Live Event
SANS Abu Dhabi 2016	Abu Dhabi, AE	Mar 05, 2016 - Mar 10, 2016	Live Event
SANS 2016	Orlando, FLUS	Mar 12, 2016 - Mar 21, 2016	Live Event
ICS410 Dubai 2016	Dubai, AE	Mar 13, 2016 - Mar 17, 2016	Live Event
SANS Secure Singapore 2016	Singapore, SG	Mar 28, 2016 - Apr 09, 2016	Live Event
SANS Atlanta 2016	Atlanta, GAUS	Apr 04, 2016 - Apr 09, 2016	Live Event
SANS Northern Virginia - Reston 2016	Reston, VAUS	Apr 04, 2016 - Apr 09, 2016	Live Event
SANS Secure Europe 2016	Amsterdam, NL	Apr 04, 2016 - Apr 16, 2016	Live Event
Threat Hunting and Incident Response Summit	New Orleans, LAUS	Apr 12, 2016 - Apr 19, 2016	Live Event
SANS Pen Test Austin	Austin, TXUS	Apr 18, 2016 - Apr 23, 2016	Live Event
SANS Secure Canberra 2016	Canberra, AU	Apr 18, 2016 - Apr 23, 2016	Live Event
ICS Amsterdam 2016	Amsterdam, NL	Apr 18, 2016 - Apr 23, 2016	Live Event
SANS Copenhagen 2016	Copenhagen, DK	Apr 25, 2016 - Apr 30, 2016	Live Event
SANS Security West 2016	San Diego, CAUS	Apr 29, 2016 - May 06, 2016	Live Event
SANS Scottsdale 2016	OnlineAZUS	Feb 08, 2016 - Feb 13, 2016	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced