

IIS LockDown Tool

- **Installation Review**
 - **Templates**
 - **Options & Actions**
 - **Undo**
 - **Log Files**
- **Running IIS Lockdown Unattended**
- **Creating custom Server Templates**

6/10/2003

© 2001-2003 Brett Hill

IIS Lockdown tool Introduction

Microsoft was in a hurry to release the IIS Lockdown tool. This was the summer of Code Red and Nimda and they had to prove in a hurry that IIS could be secured. Retroactive hotfixes just weren't cutting it. On August 23, 2001 Microsoft released the IIS LockDown Tool version 1.0 to Technet. (<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=32362>).

Some security experts complained about the lack of finesse in the tool, but IIS Administrators were pretty happy with it by and large. One of the first criticisms was not about security, but implementation—it could not be implemented via script. Sites with many servers simply could not implement the lockdown one server at a time. There were other problems as well, but the tool was quickly updated to include quite a few improvements.

This LockDown tool should not be confused with the Internet Server Security Configuration Tool which has a download filename of IISLock.exe. (Since the Internet Server Security Configuration Tool filename was IISLock, many people thought it was the IIS Lockdown tool.) Filename similarities aside, these are very different tools.

The Internet Server Security Configuration Tool has recently been removed from the Microsoft download site. This is probably a good thing. Those who used this tool were often unfamiliar with the underlying technology used by the tool: Security Templates, Consequently administrators would use the tool and break their servers' ability to do things like Terminal Services or remote

administration. Of course they were unhappy when they realized that, unlike with the IIS LockDown Tool, there is no UnDo function.

The purpose of the IIS Lockdown tool is to automate some common administrative security tasks. This was a very good thing for Microsoft to do for a number of reasons. One of these reasons is that in producing the tools, Microsoft got more in touch with what it takes to secure an IIS server in the variety of contexts they've created.

This is evidenced by the brief amount of time it took for them to produce version 2.x of the IIS Lockdown tool which included quite a few unpublished bug fixes and improvements overall. The most impressive aspect of this iteration of the IIS Lockdown tool is that, rather than attempt to fit one security configuration for all IIS installations, there are server templates installed that correspond to the various server products that use IIS (ie, Application Center, Biztalk) and roles that IIS can serve (ie, static or dynamic Web server).

You can download the latest version at

<http://www.microsoft.com/windows2000/downloads/recommended/iislockdown/default.asp>

Keep in mind the IIS Lockdown Tool was developed before ASP.net and so is not ASP.net aware. Microsoft does not have plans to update the tool.

FAQ: Should I run the IIS Lockdown Tool on IIS 6? Answer – No. This paper is intended to show how the lockdown tool works on IIS 5. It does not need to be run on IIS 6. Yes, really, I'm not kidding.

IIS Lockdown Tool History

- **Version 1 released with the Security Toolkit after Code Red**
- **Version 2 was combined with URLScan**
- **Version 2.1 improved scriptable installations and included tested templates**
- **Some early experiences with the tool caused Admins to avoid the later release**

6/10/2003

© 2001-2003 Brett Hill

IIS Lockdown Tool History

It's important to know that there are different versions of the IIS Lockdown tool available and which version you are using. They differ in both the feature set and manner in which those features are implemented. In this case, the latest is the greatest, so be certain you have the most recent version.

One key point of confusion is that between version 1 and version 2, URLScan was added to the IISLockdown tool installation executable. Be certain you understand that the IISLockdown and URLScan are two completely different programs wrapped up in the same installation routine.

Since URLScan is optionally installed by the Lockdown tool, administrators often confuse them and think they are mutually co-dependent. This is not so. You can use URLScan without running the Lockdown and you can run the Lockdown tool without installing URLScan.

Ever Hear This?

I applied the LockDown tool and IIS quit working! I had to reinstall IIS to get it working again.



Joe, MCSE Boot Camp Graduate

Poor Joe. He didn't know you can completely undo the Lockdown tool without using the Lockdown Undo function in 3 steps.

We will review those steps after a study of the tool's actions.

6/10/2003

© 2001-2003 Brett Hill

Understanding the Lockdown Tool

Knowledge is power and that is certainly true in the case of the Lockdown tool. The Lockdown tool has a very big scope in that it affects NTFS permissions, metabase configuration, and can even remove services from your server.

After a complete analysis of how the Lockdown Tool works, you will see that you can completely reverse the effects of the most significant changes very easily. That is one of the most excellent parts of this story. Consequently, even if unexpected problems arise, you won't find yourself wondering what happened to your server functionality and blaming the Lockdown tool.

IISLockd.Exe Contents

- **Urlscan_attend**
- **Runlockd unattend.doc**
- **Readme.txt**
- **Urlscan.doc**
- **Templates for each server**
- **Where are the templates stored?**

urlscan_unatten...	9/28/2001 4:19 PM	32
404.dll	11/13/2001 3:21 PM	31,080
iislockd.chm	11/6/2001 4:24 PM	37,686
iislockd.exe	11/13/2001 3:21 PM	168,528
iislockd.ini	11/6/2001 11:15 ...	11,381
readme.txt	10/13/2001 9:10 PM	302
RunLockdUnatte...	10/30/2001 8:46 PM	40,448
unattend.cmd	10/12/2001 3:17 PM	67
UrlScan.doc	10/13/2001 12:4...	74,240
UrlScan.exe	11/13/2001 3:15 PM	154,144
UrlScan.ini	10/12/2001 8:18 PM	4,137
urlscan_biztalk.ini	10/29/2001 10:4...	3,640
urlscan_commerc...	10/29/2001 10:4...	3,640
urlscan_dynamic.ini	10/29/2001 10:4...	3,919
urlscan_exchang...	10/29/2001 10:4...	3,672
urlscan_exchang...	11/1/2001 5:21 PM	3,688
urlscan_frontpag...	11/6/2001 11:16 ...	3,875
urlscan_sbs2000.ini	11/1/2001 10:36 ...	3,698
urlscan_sharepoi...	10/29/2001 10:5...	3,687
urlscan_sharepoi...	11/1/2001 5:26 PM	3,875
urlscan_static.ini	10/29/2001 10:4...	4,137

6/10/2003

© 2001-2003 Brett Hill

Inspecting the Contents of IISLockd.exe

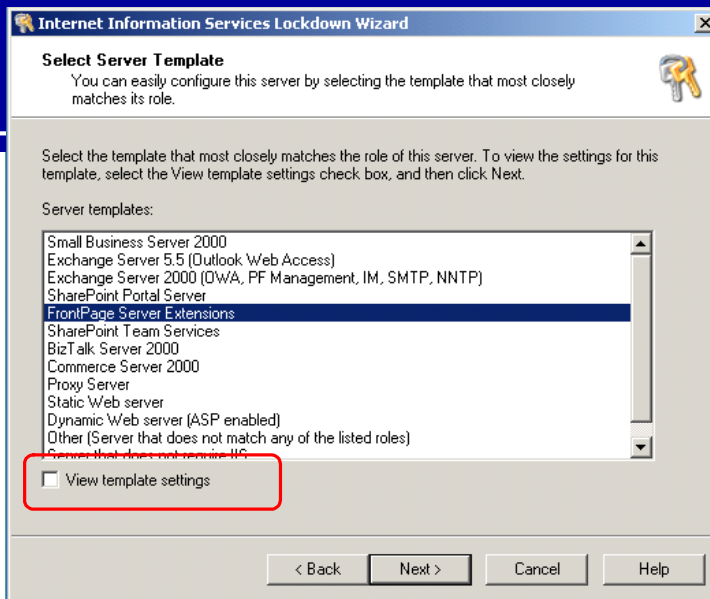
When you execute the IISLockd.exe file, it runs the Lockdown wizard, not an installation program as you might expect. In fact, if you open the .exe file with Winzip, you'll find that there is quite a lot of stuff in the .exe that you might not otherwise notice.

Documentation – You'll find the details on how to run the lockdown tool in unattended mode, which is skimpy, but it works. You will also find the very useful URLScan.doc, explaining URLScan functions.

URLscan.exe – This is version 2.0 of URLScan. You will want version 2.5, not version 2.0. It doesn't hurt to install 2.0 unless you don't know what you're doing.

IISlockd.ini – This contains details describing the options available for all the templates in the Select Server Template window. It also determines if the lockdown tool is running in unattended mode or GUI mode.

URLScan ini files – Each of these ini files is customized for a particular type of Microsoft server or server role.



6/10/2003

© 2001-2003 Brett Hill

Server Templates

Before we can explore how the lockdown tool works, you need to see how Server Templates are presented for use during the installation.

When you run the IISLockd.exe you will see a welcome screen, licensing screen and then the Select Server Template screen. This screen allows you to select a server or server role that most closely matches your needs. Once selected, you can then customize each action by selecting View template settings. If View template settings is not selected, you will skip ahead to a list of actions that are about to occur.

The Server Template listings and their default actions are all defined in the IISLockd.ini. You can create your own server templates so you can modify this list any way you wish. For example, you may find it wise to create a template that works for your situation and remove all other choices.

I suggest that you select the template that most nearly approximates your needs and then check View template settings. *This is very important.* If you do not check View template settings, the wizard will apply the settings it thinks you need. You need to verify that these settings are going to work for you before you run the Lockdown tool.

Examining the IISLockd.ini file

The IISLockd.ini has a relatively simple construction. It is composed of various sections.

Info section

The [Info] section is the first part of the IISlockd.ini file and has only a few items, but they are very important items

```
[Info]
```

```
ServerTypesNT4=sbs4.5, exchange5.5, frontpage, sharepoint_teamservices, proxy, staticweb, dynamicweb , other, iis_uninstalled
```

```
ServerTypes=sbs2000, exchange5.5, exchange2k, sharepoint_portal, frontpage, sharepoint_teamservices, biztalk, commerce, proxy, staticweb, dynamicweb, other, iis_uninstalled
```

```
UnattendedServerType=frontpage
```

```
Unattended=FALSE
```

```
Undo=FALSE
```

- ServerTypesNT4 is the list of server templates shown when the tool is run on NT4.
- ServerTypes is the list of server templates shown when the tool is run on Windows 2000.
- UnattendedServerType determines which server template is used if the lockdown tool is run in attended mode
- Unattended is a TRUE/FALSE switch that turns on and off unattended installation.
- Undo is a TRUE/FALSE switch that allows you to run an unattended Undo.

If you want to add your own template, you would simply add an entry to the ServerTypes list.

If you want to run the Lockdown tool in unattended mode, you set the template name for the template to be used with UnattendedServerType, set Unattended to TRUE, and run IISlockd.exe. EZ.

ServerType Settings

The rest of the ini file is composed of the default actions for each of the templates named in the ServerType= line of the [Info] section. The following section is the listing for Static Web Server.

```
[staticweb]
```

```
label="Static Web server"
```

```
Enable_iis_http=TRUE
```

```
Enable_iis_ftp= FALSE
```

```
Enable_iis_smtp= FALSE
Enable_iis_nntp= FALSE
Enable_asp= FALSE
Enable_index_server_web_interface= FALSE
Enable_server_side_includes= FALSE
Enable_internet_data_connector= FALSE
Enable_internet_printing= FALSE
Enable_HTR_scripting= FALSE
Enable_webDAV= FALSE
Disable_Anonymous_user_system_utility_execute_rights= TRUE
Disable_Anonymous_user_content_directory_write_rights= TRUE
Remove_iissamples_virtual_directory=TRUE
Remove_scripts_directory=TRUE
Remove_MSADC_virtual_directory=TRUE
Remove_iisadmin_virtual_directory=TRUE
Remove_iishelp_virtual_directory=TRUE
UrlScan_Install=TRUE
UrlScan_IniFileLocation=urlscan_static.ini
AdvancedSetup =
UninstallServices=FALSE
```

Most of these switches are easily recognizable as controls for features of the lockdown and correspond to elements in the GUI for lockdown tool. We will examine the actions taken by each a bit later. A few deserve explanation:

- The name for the template, in this case [staticweb] must exactly match the entry in Servertypes in the [Info] section.
- The “label=” definition determines what is displayed in the Select Server Template listing. This is where you would say “Atlanta IIS DMZ” for example if you were creating your template.
- Urlscan_Install= TRUE / FALSE / DISABLED. TRUE or FALSE sets the initial checkbox value on or off for “Install URLScan filter on the server”. DISABLED makes the checkbox unavailable.
- Urlscan_iniFileLocation= associates a specific URLScan template with this template. If Urlscan is to be installed either in the GUI or unattended, you will want to make certain this correctly designates a customized URLScan template. By the way, you WILL want to customize your URLScan template..
- The AdvancedSetup switch controls the “View Template Settings in the user interface and setting has multiple possible values:
 - Required: View Template Settings is not available. The user must view each lockdown setup screen.

- NotAvailable: View Template Settings is not available. The user cannot change the template settings defined the iislockd.ini file.
- (Blank): If AdvancedSetup has no value specified, the user is allowed to choose View Template Settings if they desire. The default is cleared – do not view template settings.

Running IISLockD.exe

- **Welcome, License, Templates**
- **Lockdown options available with FPSE template with view template options enabled**

6/10/2003

© 2001-2003 Brett Hill

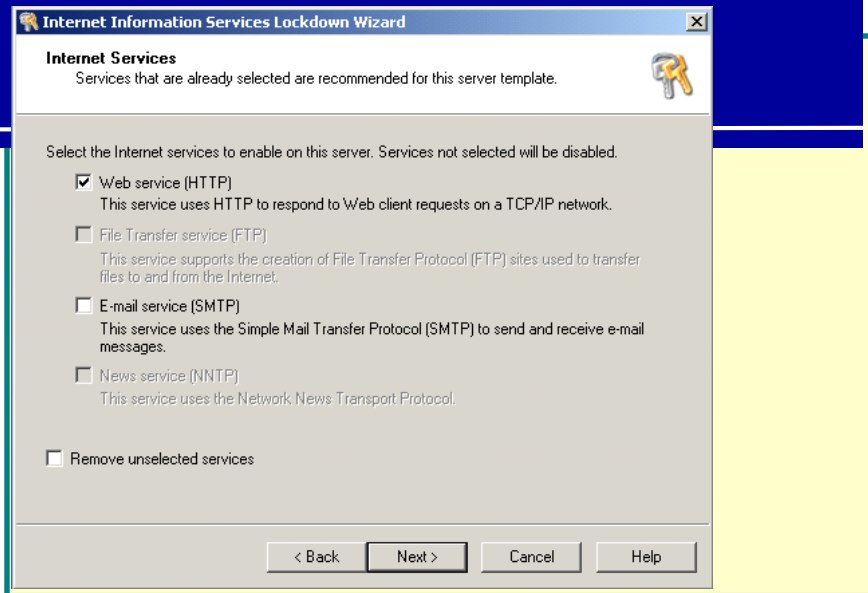
Running IISLockD.exe

When you first run the lockdown tool, you are presented with a welcome screen, a license agreement and then the Select Server Templates screen which we have covered in detail.

For the rest of the section, we are going to walk through the IIS Lockdown options available if you selected the FrontPage Server Extensions template with View template settings option enabled.

As mentioned earlier, the View template settings option allows you to review each option available in the lockdown tool. As we encounter these choices, I will explain how each works so you can make a determination about the suitability of each option.

After selecting the FrontPage Server Extensions template, click View Template settings and then click Next.



6/10/2003

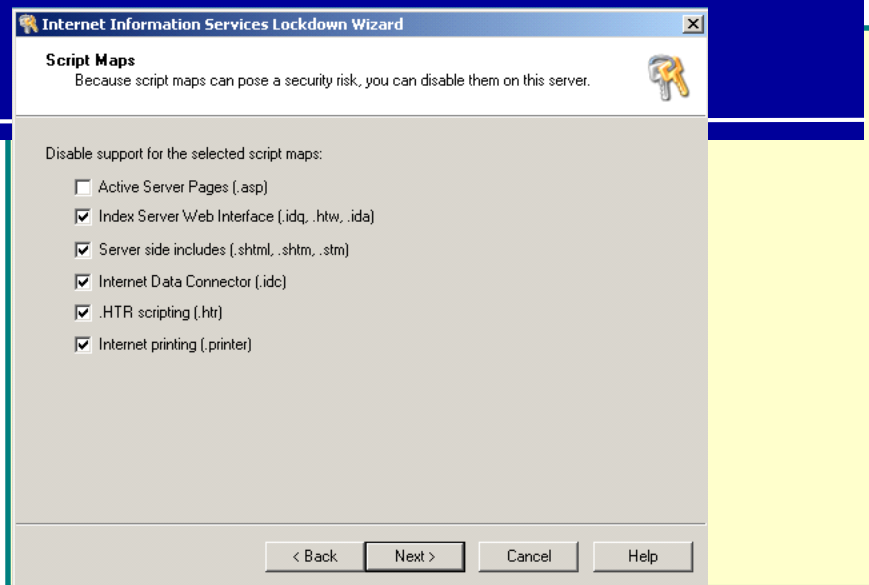
© 2001-2003 Brett Hill

Internet Services

On the Internet Services window you can disable any of the internet services you don't require. Any disabled services will be set to Disabled in the Services snap-in so it cannot be started.

Note the box "Remove unselected services." I like this option of course since a server is more secure with a service completely removed than set to disabled. However, there can be times when you want to temporarily enable a service, then turn it off again.

Click Next to show the Script Maps options.



6/10/2003

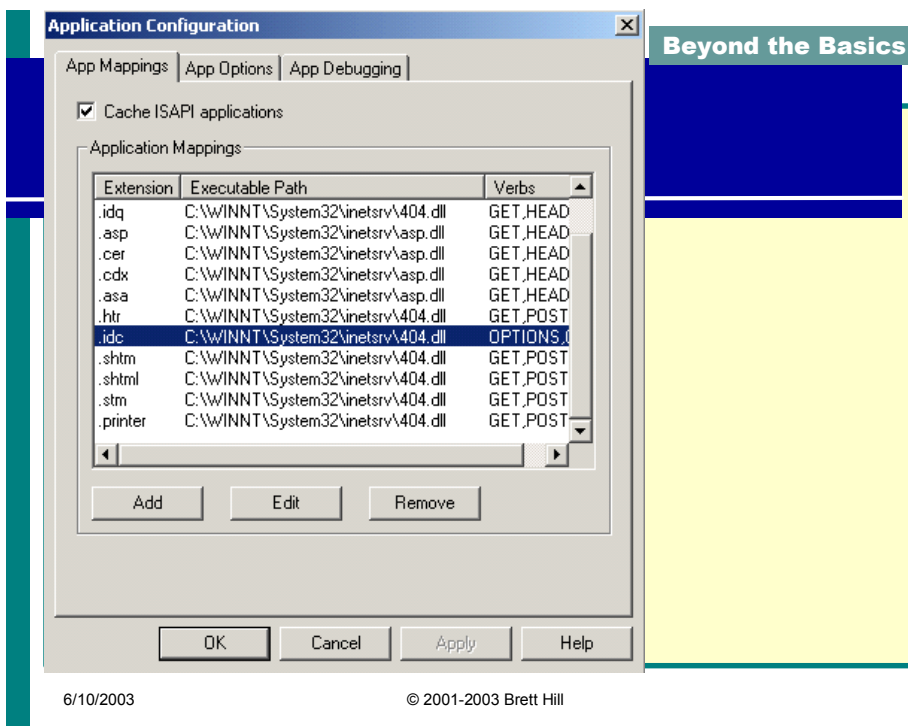
© 2001-2003 Brett Hill

Script Maps

The Script Maps window allows you to select which scripting engines you wish to enable. This is an **EXTREMELY** important setting. How the lockdown tool goes about doing this is quite clever, as it solves two problems inherent with disabling application mappings. We will review that a bit later.

Interestingly, the user interface has pulled a switch on you. In the previous window, you selected the Internet services that you wanted enabled. On this screen, you select the services you **DO NOT** want enabled.

What is most important is how the IIS Lockdown tool achieves securing these mappings.

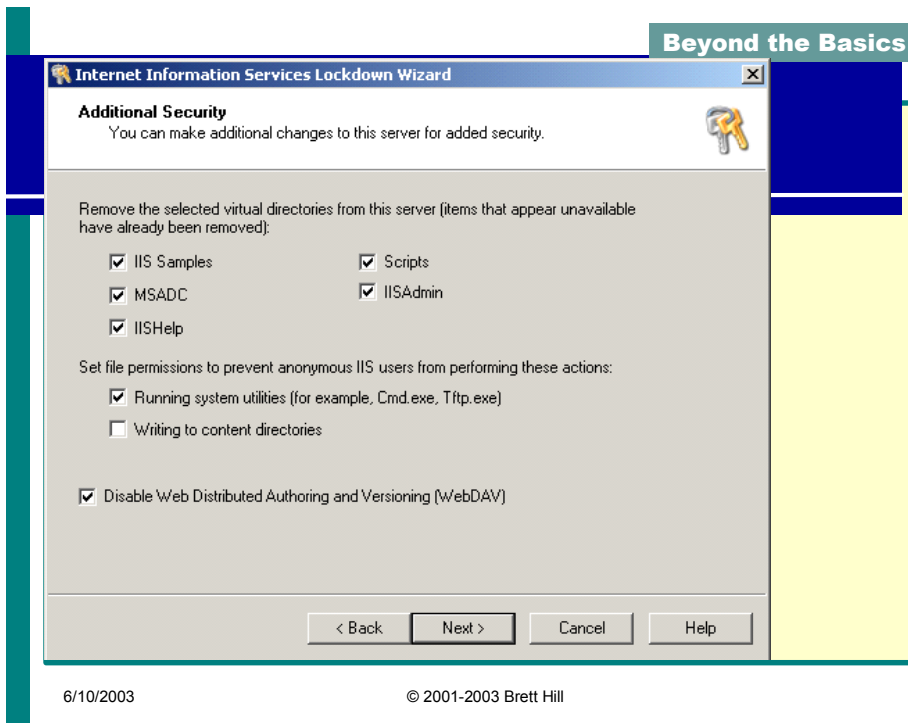


Dead End Application Mappings

As you may recall from the Disable Web Printing demonstration, removing script mappings is not always as easy it seems. In some cases they can reappear. Microsoft is a large company and any product team can add a script mapping if they deem it necessary to make their product work. So, for example, if you install Index Server, the index server application mappings reappear, even if you removed them.

Despite these facts, most security experts recommend that you remove unwanted application mappings. The IIS LockDown tool, disables these application mappings, but does not remove them. This is accomplished by mapping the file extensions to an error message provided with the IIS Lockdown tool, 404.dll located in the Winnt\system32\inet\404 folder. The anonymous account requires execute permission on this folder, and by default, will have it.

In this way, if an index server .idc file is called from a URL or a hacker tries to exploit a printer buffer overflow, an error is returned to the client. Since the mappings still exist, installation programs are not likely to add them. Clever!



Additional Security

After the Script Maps windows, you are presented with the Additional Security window which has three basic sections. Each of them is very important, so pay attention.

Remove the selected virtual directories

In the first section, you select the Virtual Directories that will be removed from the default Web site. This does not remove the underlying content. Some security critics really came down on Microsoft for not removing the files from the server. I agree that there should be an option, like there is on the services page to remove services, to remove unneeded content. However, this is still an excellent tool.

You can and should remove ALL these virtual directories on any server you wish to secure.

IISAdmin and the Administrative Web Site

In the figures on page 49, notice that the Administrative Web site has been removed from the server by the lockdown tool. We did not ask the tool to do that. We asked it to remove the IISAdmin Virtual directory. That happened too, but the tool took a few liberties here.

If you want the Admin Web site back, you can create one easily enough since the files are still present in `winnt\system32\inetsrv\iisadmin`. On a high security Web server, remove this folder.

IIS Samples

The Sample Web Files are located in \Inetpub\iissamples. There is a virtual directory mapped to this location called IISSamples in the default Web site. The default NTFS permissions on the IISSamples folder are Everyone Full control. It contains scripts such as Metaback.vbs and Mkwwebsrv.vbs that only administrators should access.

It should be noted that even though the IUSR account has NTFS permissions to run these scripts by default, such an effort would fail since the IUSR does not have rights to the metabase.

The IIS Lockdown tool will remove the IISSamples virtual directory, but the IISSamples folder and files still reside on the hard drive. In theory, they cannot be accessed from the default Web site, but that is just a theory.

It is recommended that these files be removed on a secure server or at least secured with NTFS permissions if you wish to keep them. The Lockdown tool will tighten the permission of this folder if you select to secure Web content.

Scripts

The Scripts virtual directory is found in the Default Web Site. It maps to \Inetpub\Scripts. This folder has Everyone Full Control by default. However, there is nothing in it by default. The Scripts virtual directory is marked for Scripts and Executables in the IIS snap-in, but the Web based permissions deny Write and Read access.

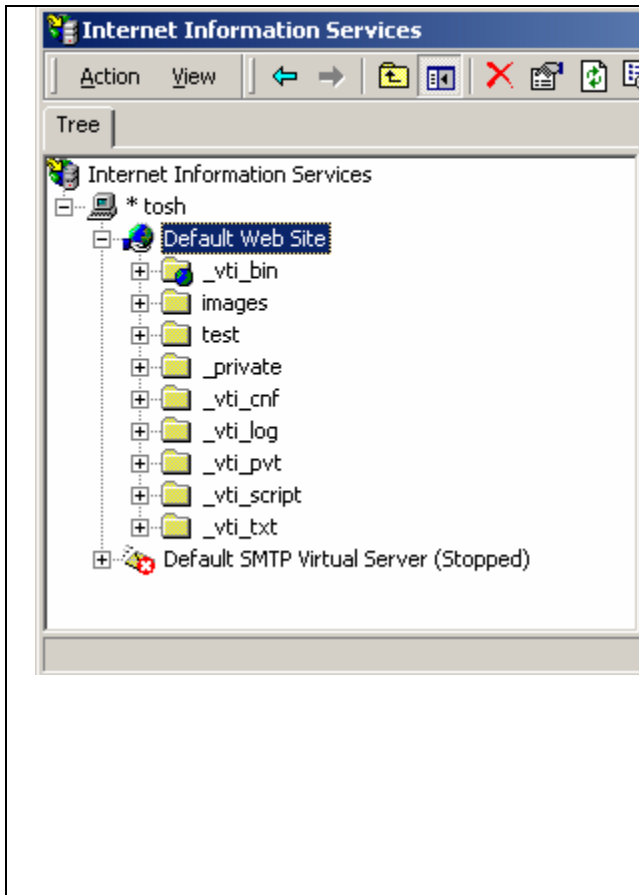
The IIS LockDown tool removes the Script virtual directory from the Default Web site, but does not remove the folder itself. Additionally, NTFS permissions are left at Everyone Full Control, if you do not select to secure Web content. I would suggest removing this folder or changing NTFS permissions so the Anonymous user cannot write to this folder.

The Scripts folder is a favorite target for hackers and was one of the primary means by which Nimda managed to get a hold in IIS servers.

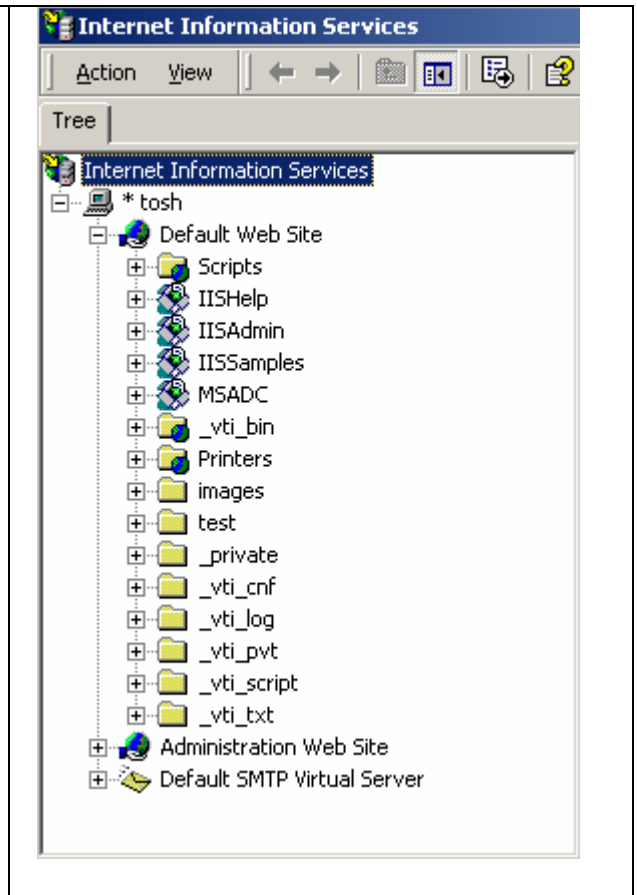
MSADC

See the pattern here? Again there is a virtual directory in the Default Web Site, the MSADC directory in this case. The MSADC virtual directory is mapped to %Systemroot%\program files\common files\system\msadc. The Users group, which includes the Anonymous user, has Read and Execute rights to this folder by default and this is not changed by this setting of the Lockdown tool. The Lockdown tool will change the permission of this folder automatically if you choose to secure Web content folders.

If you do not require the features of the MSADC programs (typically RDS), it is strongly recommended that this folder be deleted.



After IIS Lockdown



Before IIS Lockdown

Set file permissions to prevent anonymous IIS users from...

1. Running system utilities

The ability of the Lockdown tool to prevent anonymous users from gaining access to system utilities may be its most useful feature. When this option is selected, the LockDown tool changes NTFS permissions on hundreds of files. You cannot customize the file listing but you can review the changes in the IISLockdown logs.

2. Writing to content directories

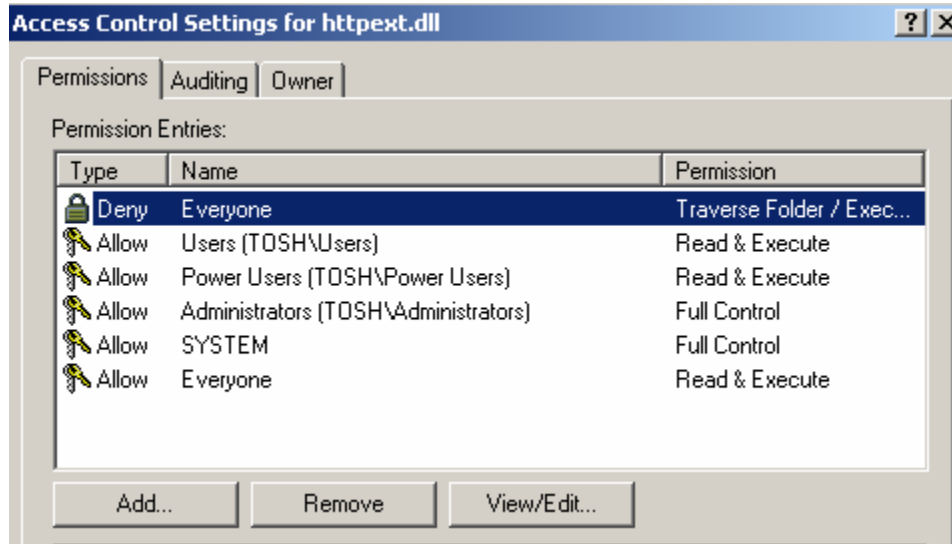
Another feature of the IIS lockdown tool is the ability to disable the ability of the Web Anonymous Users Group and the Web Application group to Write to the web server content folders. The Lockdown tool will set the Deny Write permission for these groups on files and folders and virtual directories that are part of the Web content tree.

This is a very good idea since it forces you to specifically enable permissions in order for the anonymous user to be able to write to the server.

3. Disable WebDAV

WebDAV is provided by HTTPEXT.DLL located in %Systemroot%\Winnt\System32\inetrv. By default, Everyone has the ability to Read and Execute this file. The IISLockdown tool

attempts to disable WebDAV by assigning the Deny Execute permission to Everyone for HTTPEXT.DLL.



I do not recommend using this technology. You are still able to use WebDAV to implement PUT and DELETE requests, even if the ACLs are set. These capabilities are evidently enabled elsewhere in IIS.

Instead, take advantage of a new Registry entry introduced by the Windows 2000 SRP1 (as per Q307934) or SP3. At the Registry key,

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters

Add the value:

Value name: DisableWebDAV
Data type: DWORD
Value data: 1

This is much better than messing with the ACLs on HTTPEXT.DLL. You can also disable WebDAV with URLScan.

Bottom line: don't use this feature of the Lockdown tool.

A Closer Look at Permissions

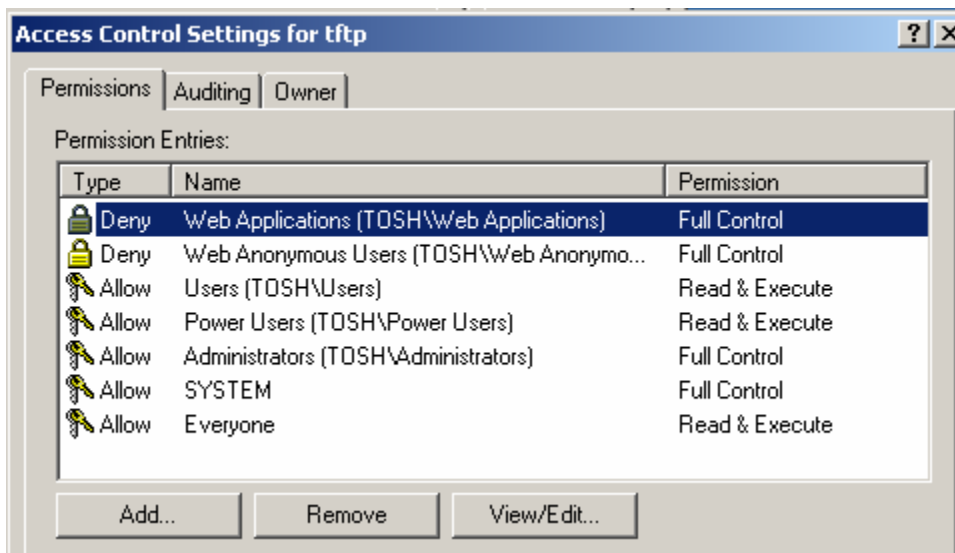
- **Web Anonymous Users Group**
- **Web Applications Group**
- **Recovering from Lockdown Permissions Changes**
- **Making Users Anonymous Equivalents**

6/10/2003

© 2001-2003 Brett Hill

A Closer Look at Permissions

In addition to being a useful security measure, the method used to implement securing NTFS for the Web Anonymous users and Web Applications group can potentially be very useful in troubleshooting and administration.



Web Anonymous Users Group

For many years, Microsoft has taught that the way to manage NTFS permissions is to create local groups, add users (and global or universal groups) to local groups, and assign permissions to the local groups. Kudos to Microsoft for practicing what they preach in this instance.

Instead of assigning permissions to the IUSR account, the Lockdown tool creates a Web Anonymous Users local group which contains the IUSR account. The Web Anonymous Users account is assigned the Deny Write permission on Web content and the Deny Full Control permission on selected administrative tools, if those options are enabled during the lockdown.

In the above Access Control list you can see that TFPT can no longer be run by the Anonymous user. Of course, this won't help much with a buffer overflow if the application is running in the System account, but in most cases your application will be running out of process as the IWAM user..

Web Applications Group

This was quite surprising to find in the lockdown tool, since it has not at all related to anonymous users. Nevertheless, this feature is enabled if you select to “prevent anonymous IIS users from performing...actions”.

The Lockdown tool creates a Web Applications local group which contains the IWAM account. The Web Applications account is assigned the Deny Write permission on Web content and the Deny Full Control permission on selected administrative tools, if those options are enabled during the lockdown.

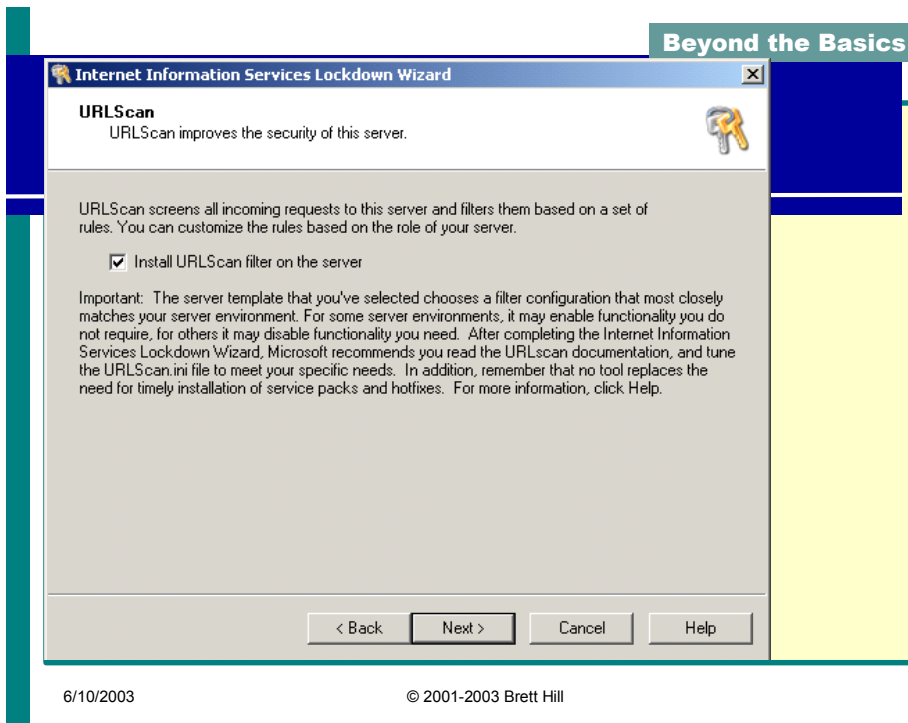
Returning to the example above, you can see that the Web Applications group has been denied Full Control to the TFPT executable. In the event that a buffer overflow attack occurs in an application running Out-of-Process, the IWAM account will not have privileges to execute many administrative tools. In this case, had TFPT failed to launch, Nimda would have been defeated even if the buffer overflow was successful.

Recovering from Lockdown Permissions Changes

If the IIS Lockdown tool permissions break your server, you have only to remove the IUSR and IWAM accounts from these two groups to return the server to its previous effective state. Anyone claiming that the lockdown tool permissions broke their server and that they had to reinstall is simply uninformed.

Making Users Anonymous Equivalentents

Since Microsoft kindly used local groups to manage these permissions, you can easily make a user or group “anonymous equivalentents.” You need only to add the user or group to the Anonymous Web User local group. This is handy for groups like the ASPNET user in ASP.net.



URLScan

This wordy paragraph that is labeled “Important” is in fact important. Your server can be completely disabled when using an incorrectly configured URLScan.ini file. This is easy to correct (see TIP below), but I have this radical belief that your server can be secure and functional. Recall that the IISLockdown.ini controls the URLScan template installed when this option is selected.

IMPORTANT: There is a newer version of URLScan than the one contained in the IISLockd.exe file. You will want to use URLScan 2.5 which can be found at <http://www.microsoft.com/downloads/release.asp?ReleaseID=38019>

You can extract the URLScan executable and templates from the IISLockd.exe and install them separately from the IISLockdown tool.



TIP

URLscan installs as an ISAPI filter at the master Web properties level. If you do install URLScan and suspect it is causing problems with your server, you need only to remove it from the Filters listing and restart the server to restore “normal” functioning. It does not modify any other settings on your server. Consequently, URLScan cannot break your server in any permanent sense.

Reviewing the Lockdown Actions

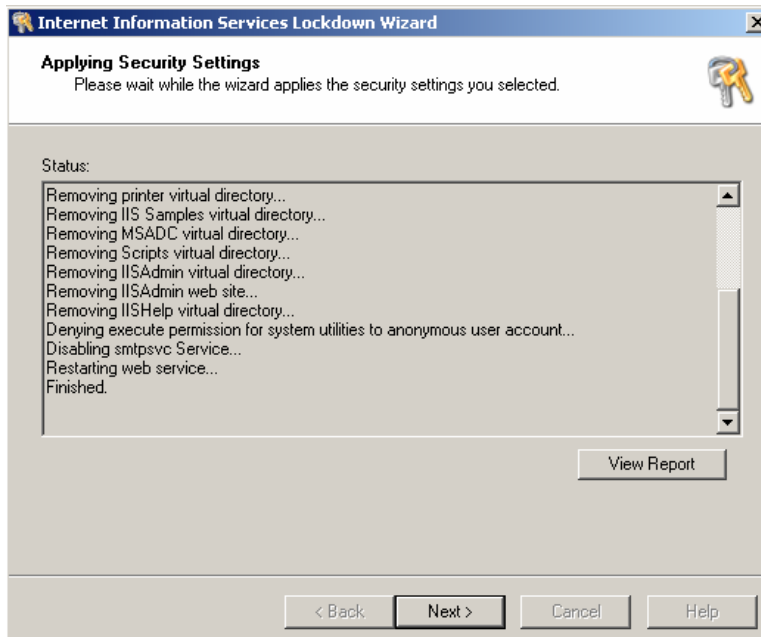
- **Applying Security Settings Screen View Report**
- **Metabase Backup**

6/10/2003

© 2001-2003 Brett Hill

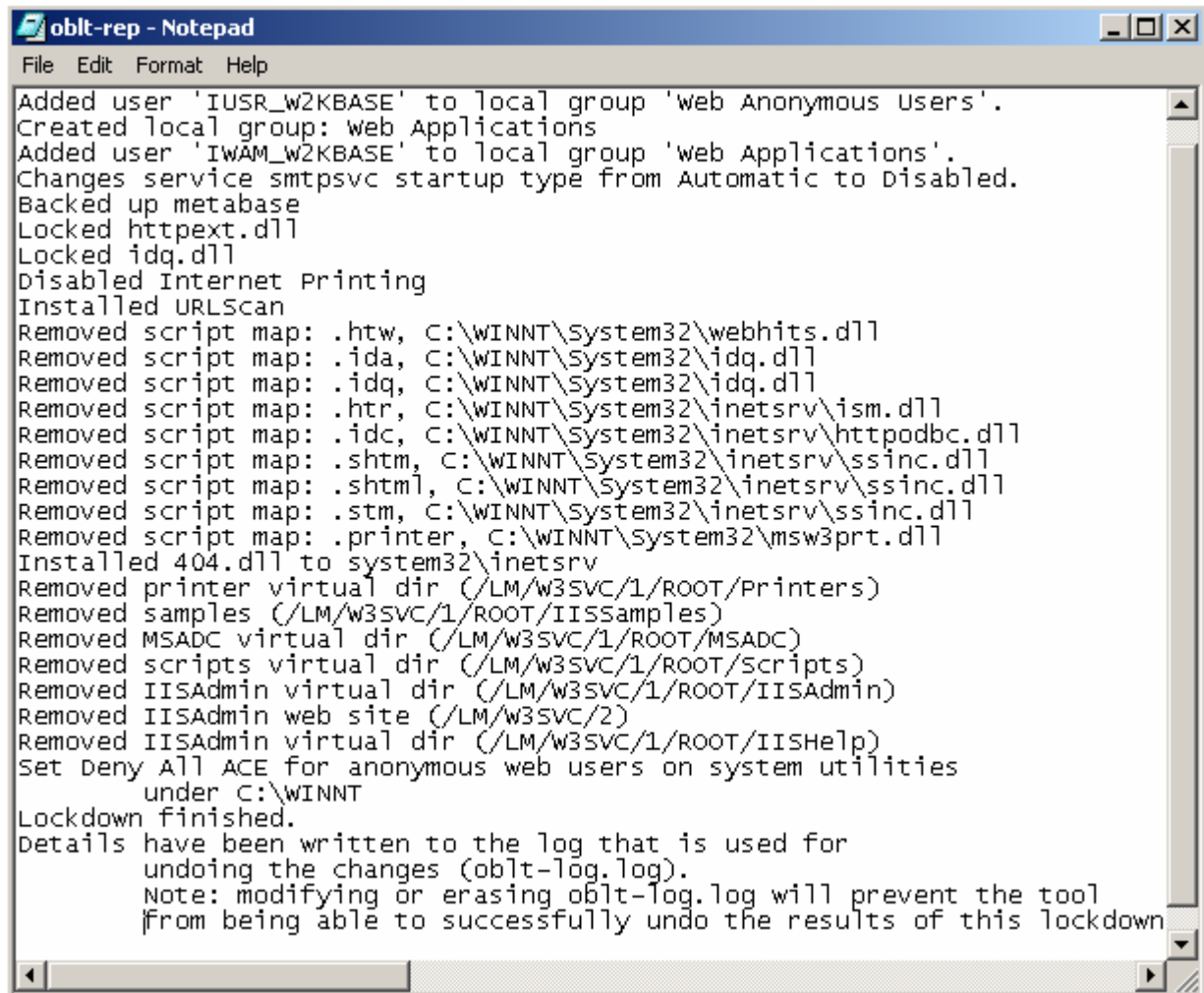
Reviewing the Lockdown Actions

After you click **NEXT**, you'll see a confirmation screen which will review your settings. Clicking **NEXT** again, starts the lockdown process.



At this point, you might be thinking, “Oh, my gosh, what just happened?”

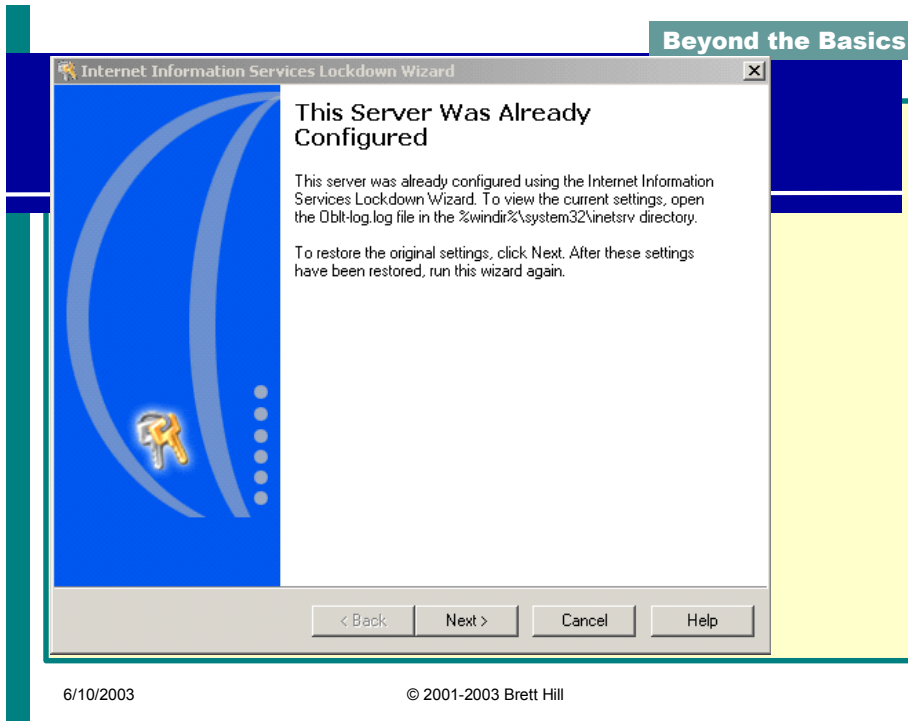
You can view a summary of events with the View Report button as follows:



```
oblt-rep - Notepad
File Edit Format Help
Added user 'IUSR_w2KBASE' to local group 'web Anonymous Users'.
Created local group: web Applications
Added user 'IWAM_w2KBASE' to local group 'web Applications'.
Changes service smtpsvc startup type from Automatic to Disabled.
Backed up metabase
Locked httpext.dll
Locked idq.dll
Disabled Internet Printing
Installed URLScan
Removed script map: .htw, C:\WINNT\System32\webhits.dll
Removed script map: .ida, C:\WINNT\System32\idq.dll
Removed script map: .idq, C:\WINNT\System32\idq.dll
Removed script map: .htr, C:\WINNT\System32\inetsrv\ism.dll
Removed script map: .idc, C:\WINNT\System32\inetsrv\httpodbc.dll
Removed script map: .shtm, C:\WINNT\System32\inetsrv\ssinc.dll
Removed script map: .shtml, C:\WINNT\System32\inetsrv\ssinc.dll
Removed script map: .stm, C:\WINNT\System32\inetsrv\ssinc.dll
Removed script map: .printer, C:\WINNT\System32\msw3prt.dll
Installed 404.dll to system32\inetsrv
Removed printer virtual dir (/LM/W3SVC/1/ROOT/Printers)
Removed samples (/LM/W3SVC/1/ROOT/IISamples)
Removed MSADC virtual dir (/LM/W3SVC/1/ROOT/MSADC)
Removed scripts virtual dir (/LM/W3SVC/1/ROOT/scripts)
Removed IISAdmin virtual dir (/LM/W3SVC/1/ROOT/IISAdmin)
Removed IISAdmin web site (/LM/W3SVC/2)
Removed IISAdmin virtual dir (/LM/W3SVC/1/ROOT/IISHelp)
Set Deny All ACE for anonymous web users on system utilities
under C:\WINNT
Lockdown finished.
Details have been written to the log that is used for
undoing the changes (oblt-log.log).
Note: modifying or erasing oblt-log.log will prevent the tool
from being able to successfully undo the results of this lockdown
```

Metabase Backup

One of the built in actions of the tool is to back up the metabase. In the event that you “undo” the IIS Lockdown settings, the metabase will be restored as well. Changes you made in between the Lockdown and the Undo will be lost.



Automatic Undo

The LockDown tool allows you to undo the previous lockdown. This reverses the settings enforced by the tool, and field testing reports that it seems to work very well. Be advised that this will restore your metabase to the state it was in before you ran the tool. If you ran the tool, made changes to the metabase, then ran Undo, those changes would be lost.

To Undo, simply run IISLOCKD again.

Also, in testing, the Internet Services Manager would sometimes incorrectly report the current structure of the metabase. It is necessary to reboot the server in order to be assured that all this is fully in sync. I strongly recommend a reboot of the server any time the metabase is replaced.

Getting Past the UNDO

There may be the occasion when you want to run the Lockdown tool but your server thinks it has already been run. You can cause the Lockdown tool to think it has never been run by deleting the files

```
Winnt\system32\inetsrv\Obflt-rep.log
Winnt\system32\inetsrv\metaback\Obflt-once.md0
Winnt\system32\inetsrv\metaback\Obflt-mb.md0
```

Be advised that the .md0 files are metabase backups and can be used to restore your IIS configuration to its pre-lockdown state.

See <http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q316327&> for details.

3 Steps to Reverse the Lockdown

- **Remove the URLScan ISAPI filter from the ISAPI Master Properties**
- **Remove user accounts from the Lockdown Groups**
 - **Remove the IUSR account from the Web Anonymous Users Group**
 - **Remove the IWAM account from the Web Applications Group**
- **(Optionally) Restore the metabase**

6/10/2003

© 2001-2003 Brett Hill

Manual Undo:

Three Steps to Reverse the Lockdown

Since Microsoft was rather thoughtful about the way Lockdown was implemented, you can easily reverse the effects of the lockdown without running the automatic Undo. This may be quite useful to you if you have some part of the lockdown you want to fine tune.

- To nullify the effects of the NTFS permissions changed:
Remove the IUSR account from the Web Anonymous Users Group.
Remove the IWAM account from the Web Applications Group.
- To nullify the effects of URLScan:
Remove URLScan from the WWW Master Properties ISAPI Filter list.
- To restore the application mappings and virtual directories:
Either manually restore the mappings or restore the metabase.

There are only two other items:

- If you choose to disable WebDAV, then remove the DENY permission on HTTPEXT.DLL.
- If you choose to disable services, then change the service startup back to either Automatic or Manual as you require.

Reviewing the Logs

- **The Lockdown tool keeps a detailed log of its actions in %systemroot%\system32\inetsrv.**
- **After a lockdown:**
 - **oblt-rep.log, a summary report**
 - **oblt-log – details of the last lockdown**
- **After an Undo:**
 - **oblt-undo.log**
 - **When you undo, the oblt-log becomes oblt-undo.log**
 - **oblt-undone.log is a log of what occurred during the undo**
- **An examination of the log files shows exactly what files had permissions changed and other actions such as backing up or restoring the metabase.**

6/10/2003

© 2001-2003 Brett Hill

Reviewing the Logs

The Lockdown tool keeps a detailed log of its actions in %systemroot%\system32\inetsrv. The log files are named:

After a lockdown:

- oblt-rep.log, a summary report
- oblt-log – details of the last lockdown

When you Undo a lockdown:

- oblt-undo.log –When you undo, the oblt-log becomes oblt-undo.log
- oblt-undone.log- a log of what occurred during the undo

An examination of the log files shows exactly what files had permissions changed and other actions such as backing up or restoring the metabase.

Creating Custom Templates



6/10/2003

© 2001-2003 Brett Hill

Creating Custom Templates

Now that you've had a complete walkthrough of the capabilities and mechanics of the Lockdown tool, let's create a custom template. This allows you to customize functionality for your organization and eliminate configurations that could potentially break your server.

<This is a lab we do in training. It has been removed since it won't work for you without the required labfiles>

Summary



6/10/2003

© 2001-2003 Brett Hill

Summary

Overall, I find that The IIS LockDown tool is quite strong. You can very quickly remove access to default locations, secure administrative tools from the anonymous user, disable selected ISAPI filters, and disable write access for the anonymous account.

While overall the Lockdown is useful, keep the following details in mind:

- After running the tool, you should manually secure the NTFS permissions for any folder in Inetpub as well as remove the Scripts, IISamples and MSDAC folders.
- Additionally, securing the administrative tools from use by the Anonymous account is important; however, in the event of a buffer overflow attack, the attacker may be using the System account. Consequently, while protecting these tools from anonymous access is essential, it is insufficient. Recommendations for securing these files can be found in the *Preparing W2K* module.
- Denying write access to the anonymous user may break Web based database applications as well as some Front Page Server Extensions functions. The FPSE permissions model conflicts with the IISLockdown model in that FPSE assigns permissions on a user by user basis whereas the Lockdown tool users groups. Further testing remains to be done to see how compatible the Lockdown tool permissions model is with FrontPage Server Extensions.

- Denying write permissions to the Web Applications group may cause some problems with out of process applications or COM objects that do not properly impersonate users.
- I don't recommend disabling WebDAV with the Lockdown tool. You are more secure using the registry entry referenced in this module as well as URLScan
- Be careful implementing the default URLScan templates for any server. Check the KB for updates and be sure you make any necessary modifications.

