



Internet Information Server

Bhupendra Kumar

CERT-In

Department of Information Technology

Ministry of Communications & Information Technology

Electronics Niketan, 6 C.G.O. Complex

New Delhi- 110 003



→ COMMON ATTACK ON IIS
HARDENING
COMMON LOGS
TOOLS

"Securing Internet Information Server"

COMMON ATTACKS

- ➔ **Remote Data Services (RDS)**
- ➔ **Unicode (Nimda)**
- ➔ **Unicode (Code Red)**
- ➔ **Directory Enumeration**
- ➔ **Path Truncation**
- ➔ **sadmin/IIS Worm**



ANATOMY OF ATTACK

Act 1: The Scan:- running a port scan to detect the open HTTP and HTTPS ports

Act 2: Information Gathering

Act 3: Testing:- the application scripts or dynamic functions of the application, looking for development errors

Act 4: Planning the Attack

"Securing Internet Information Server"

COMMON ATTACKS

Path truncation.

WebInspect truncates paths, looking for directory listings or unusual errors within each truncation.

For example, a link like the following example may exist on your site:

`/customers/id/993/details.html`. WebInspect will begin truncating the path looking for vulnerabilities within each truncation, as follows:

`/customers/id/993/`

`/customers/id/`

"Securing Internet Information COMMON ATTACKS Server"

sadmind/IIS worm

Microsoft IIS servers that are successfully compromised exhibit the following characteristics:

Modified web pages that read as follows:

fuck USA Government

fuck PoizonBOx

contact:sysadmcn@yahoo.com.cn

Sample Log from Attacked IIS Server

```
2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 GET /scripts/../../../../winnt/system32/cmd.exe /c+dir 200 -
```

```
2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 GET /scripts/../../../../winnt/system32/cmd.exe /c+dir+..\ 200
```

```
-
```

```
2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 GET
```

```
/scripts/../../../../winnt/system32/cmd.exe/c+copy+\\winnt\system32\cmd.exe+root.exe 502 -
```

```
2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 GET /scripts/root.exe /c+echo+<HTML code inserted here>../../../../index.asp 502 -
```

COMMON ATTACKS

SIGNATURES

→ /passwd

→ /dir

→ /tftp

→ /ftp

→ /Admin.dll

→ /default.ida

→ /iisstart.asp

→ /iisadmpwd

→ /cgi-bin

→ /admin

→ /passwd

→ /dir

→ /tftp

→ /ftp

→ /Admin.dll

→ /default.ida

→ /iisstart.asp

→ /iisadmpwd

→ /cgi-bin

→ /admin

COMMON ATTACK ON IIS

→ HARDENING

COMMON LOGS

TOOLS

Secure Installation Planning

- Security Checklists
 - Useful, however Security Checklists DO NOT equal System Security
- Baseline Checklists
 - Microsoft, CERT-In, SANS, Pentasafe, etc.
- Build machines offline or with private IP addresses
- Remove the default web site & create a new web site
- Install on a partition other than OS

Web-based Permissions

- General Access Permissions
 - Recommended to leave General Access Permissions other than read disabled
 - Leave Script Source Access disabled
 - Leave Write disabled
 - Leave Directory Browsing disabled
 - Leave Execute permissions set to none
- Execute Permissions
 - Recommend setting on a per-web-site and per-directory basis
 - If executables (.exe, .dll) are required, use Scripts and Executables setting
 - Otherwise, if scripts (.asp) are required, use Scripts setting
 - Otherwise, leave Execute Permissions to the setting of None

SSL

- Protocol for encrypting network traffic
- Operates on the transport layer port 443
- How it works:
 - Client connects to server
 - Server indicates need for SSL
 - Client and server exchange crypto keys
 - Secure session begins
- Obtain certificates from Thawte

Set Appropriate ACLs on Virtual Directories

- Application dependent, but rules of thumb are:

File Type	Access Control Lists
CGI (.exe, .dll, .cmd, .pl)	Everyone (RX) Administrators (Full Control) System (Full Control)
Script files (.asp)	Everyone (RX) Administrators (Full Control) System (Full Control)
Include files (.inc, .shtm, .shtml)	Everyone (RX) Administrators (Full Control) System (Full Control)
Static content (.txt, .gif, .jpg, .html)	Everyone (R) Administrators (Full Control) System (Full Control)

Disable or Remove All Sample Applications

Samples should never be installed on a production server
Default locations for some of the samples:

Sample	Virtual Directory	Location
IIS Samples	\IISamples	c:\inetpub\iissamples
IIS Documentation	\IISHelp	c:\winnt\help\iishelp
Data Access	\MSADC	c:\program files\common files\system\msadc

Disable WebDAV

Enabled by default

Allows for remote file management via HTTP

Remove the IISADMPWD Virtual Directory

- ➔ Remove the IISADMPWD Virtual Directory if it exists
- ➔ Allows you to reset Windows NT and Windows 2000 passwords
- ➔ Designed for intranet-only scenarios
- ➔ Isn't installed by default install of IIS 5, but is not removed when upgrading a IIS 4 server to IIS 5

Remove Unused Script Mappings

- When IIS receives a request for a preconfigured filetype, the call is handled by a DLL
- If the filetype or functionality isn't required, remove the mapping using the Internet Services Manager MMC

If you don't use...	Remove this entry:
Web-based password reset	.htr
Internet Database Connector	.idc
Server-side Includes	.stm, .shtm and .shtml
Internet Printing	.printer
Certificate Request	.cer
Index Server	.htw, .ida and .idq

Check <FORM> and Querystring Input ASP Code

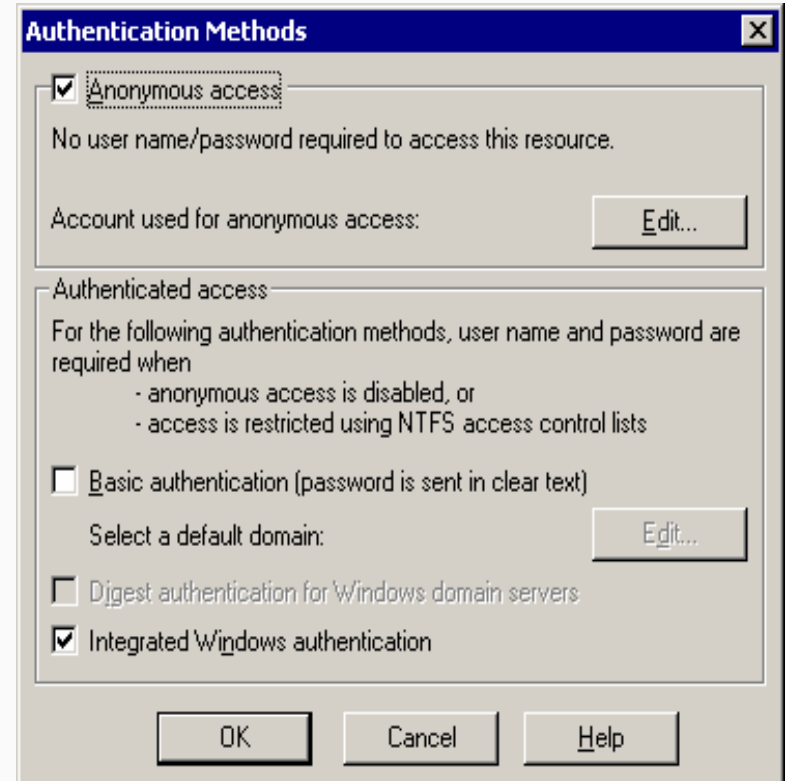
- Many sites use user input to call other code or build SQL statements directly
- There are attacks where user input is treated incorrectly as valid input allowing unintended access
- You should always check each <FORM> input and query string before passing it on to another process or method call that might use an external resource such as the file system or a database.

Disable Parent Paths

- Parent Paths allows use of “..” in calls to functions as MapPath
- Enabled by default
- Recommend to disable this
 - Select Properties of Web site root
 - Select Home Directory, Configuration
 - Open App Options tab
 - Uncheck Enable Parent Paths check box

Disable Unnecessary Authentication Types

- Anonymous
 - Default authentication method
- Basic
 - Should only be used with SSL
- Digest
 - Requires storing passwords in clear text on the domain controller
- Integrated
 - Provides a login/password dialog box, but unlike basic authentication, it encrypts the information as it is exchanged. IIS server must be a domain controller



Disable IP Address in Content-Location

- Content-Location header can expose IP addresses hidden by a firewall or proxy
- Recommend to disable this (IIS - 5)
 - Open a command window (cmd).
 - Change the directory to: inetpub\adminscripts.
 - adsutil set w3svc/UseHostName True
 - net stop iisadmin /y
 - Net start w3svc
- Another way to work around this issue is to use Active Server Pages instead of static html pages (.htm or .html) and create a custom header that sends back a specific Content-Location.

Enable Logging

- Move and rename the IIS Log files directory
- **Use W3C Extended Logging**
 - **Set the following properties:**
 - Client IP Address
 - User Name
 - Method
 - HTTP Status
 - Win32 Status (Look for error 5, Access Denied)
 - Use “net helpmsg <error #>” to decode error number
 - User Agent
 - **And if hosting multiple Web servers on single computer:**
 - Server IP Address
 - Server Port
- ➔ **Make sure the ACLs on the IIS-generated log files:**
 - Administrators (Full Control)
 - System (Full Control)
 - Everyone (Read, Write, Change)

Counter Measures

- Physical barrier
 - Place behind a Firewall
 - Separate machines for web and database servers
- Create separate OU for web servers that is locked down via Group Policies
- Monitor and Test your web servers
 - (Think like an attacker)
- Detect rogue servers

Best Practices

- Physical barrier.
 - Place Content on a different drive
 - Use separate domains or organizational units.
- Turn off anonymous FTP **immediately**.
- Disable Unnecessary Services, Protocols and Features.
 - Remove unused virtual directories
 - Clean out scripts directory
 - Remove unused application mappings
 - Disable parent paths
- Lower your connection timeout
- Don't send detailed error messages
- Keep up-to-date – Patch your system
- ISS/ Nessus vulnerability scan of your web environment.
- Enable Security logging.
- Prevent Rouge web servers
- Monitor the audit logs daily.
- Stay Informed

COMMON ATTACK ON IIS

HARDENING

→ COMMON LOGS

TOOLS

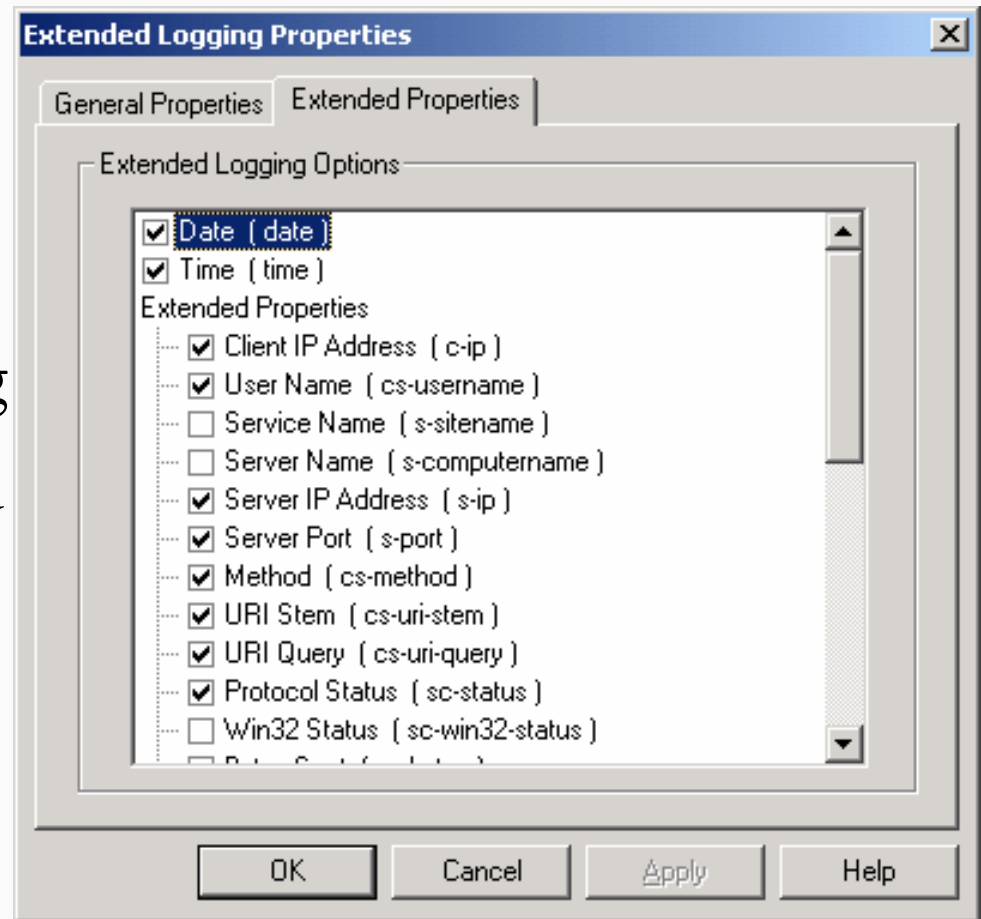
IIS Log File Specifics

Name generation

- Supports hourly, daily, weekly and monthly log file rotation and naming.
- Create a new log file based on a size threshold.
- Or if desired, the logfile can be left to grow without limit. (highly impractical approach)
- Default system log directory is “c:\winnt\system32\logfiles”,
- Each virtual web server will have its own subdirectory beneath the configured log directory.
- Web server logs are typically stored in the “W3SVC1”, “W3SVC2”, etc.
- No known way to combine multiple virtual server logs into a single file.
- IIS does not write log files line by line but rather block by

IIS LOGS

1. Internet Services Manager
 2. Select web site → Properties
 3. Check Enable Logging
 4. Properties → Extended Properties
- ◆ URLSCAN log



IIS Logs (cont.)

- **Set Appropriate IIS Log File ACLs**
 - Make sure the ACLs on the IIS-generated log files (c:\winnt\system32\LogFiles) are
 - Administrators (Full Control)
 - System (Full Control)
 - Everyone (RWC)
 - This is to help prevent malicious users deleting the files to cover their tracks.
- Create a separate Partition for Log files
- Copy logs off to a separate server to prevent tampering
- Daily, hourly
- Increase the size of your security log to 500 MB
- Configure it to only overwrite events older than 15 days if you have a once per week backup schedule.

IIS Logs - Sample

#Software: Microsoft Internet Information Services 5.0

#Version: 1.0

#Date: 2003-11-27 06:21:21

#Fields: time c-ip cs-method cs-uri-stem sc-status

06:21:21 202.141.12.50 GET /Default.htm 200

06:51:07 202.141.12.50 GET /data/australia/economy.htm 200

06:52:25 202.141.12.50 GET /scripts/root.exe 404

sc-status

1xx - continue

2xx - success

3xx - redirect (also a success)

4xx - client error (failure)

5xx - server error (failure)

Code	Description
100	Continue
200	File transfer OK
400	Invalid request
404	File not found
500	Internal server error
502	Bad gateway
503	Service unavailable
504	Gateway Time-out

COMMON ATTACK ON IIS
HARDENING

COMMON LOGS

➔ TOOLS

IIS Tools

- **Security “What If” Tool**
- **Security Configuration Tool**
- **Lockdown Tool**
- **URLScan**

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools.asp>


IIS Security "What If" Tool Screenshot

The Internet Information Services Security - Microsoft Internet Explorer

File Edit View Favorites Tools Help

← Back → Search Favorites History

Address C:\TechDocs\IIS Security\IISPerms\IISPermissions.htm Go Links >>



The Internet Information Services Security "What If" Tool (v1.05.0037)

By Michael Howard, Windows 2000 Security Program Manager (mikehow@microsoft.com)

This simple tool will help you determine what browsers, platforms, authentication schemes and server configurations will allow you to access a remote resource. Some example scenarios are listed below.

For more information on how and why these scenarios work, please refer to ["Designing Secure Web-based Applications for Windows 2000."](#) published by Microsoft Press.

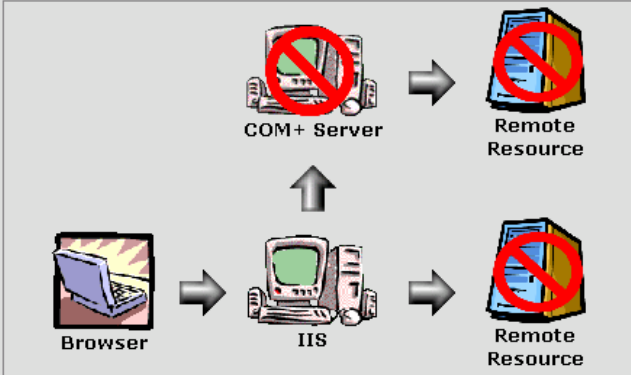
Browser: Internet Explorer 5.x
Client OS: Windows 2000
Scenario: Internet
Web Server: IIS 5 (Windows 2000, no Active Directory)
Web Auth: Anonymous (with password sync enabled)

Check Reset

Required Logon Type: Accounts must have network logon privilege.

Comment

Anonymous auth with password sync cannot delegate credentials to a remote server. Disabling password sync will enable delegation however.



COM+ Server → Remote Resource

Browser → IIS → Remote Resource

Done My Computer

IIS Security Configuration Tool Questionnaire Screenshot

The screenshot shows a web browser window titled "Windows 2000 Internet Server Configuration Tool - Microsoft Internet Explorer". The address bar shows the URL "C:\TechDocs\IIS Security\IISLock\Tool\DataEntry\Default.htm". The main content area is titled "Windows 2000 Internet Server Security Configuration Tool". On the left, there is a navigation menu with links: Home, View the README file, Build a Security Template, Microsoft Security Web Site, and About and Legal Notice. The main content area is titled "Build a Security Template" and contains a section "I wish to:" followed by a list of options with checkboxes. The options are: Remotely administer this computer using Windows Networking (checked), Remotely administer this computer over the Web (checked), Use this server as a File Transfer Protocol server (FTP) (checked), Use this server as an Internet email server (SMTP, POP3) (unchecked), Use this computer as an Internet news (NNTP) server (unchecked), Use Secure Sockets Layer/Transport Layer Security (SSL/TLS) on this server (checked), Use this computer as Telnet server (unchecked), Allow files other than static files (.txt, .html, .gif etc) and Active Server Pages to be served (checked), Use Internet Printing (unchecked), Use Server Side Includes (SSI) (unchecked), Change Windows passwords over the Web (unchecked), Use Index Server with IIS (unchecked), and Keep the Web samples (unchecked). At the bottom, there is a text input field for "Template Name:" containing "IISTemplate.txt" and a "Create Template" button.

Windows 2000 Internet Server Configuration Tool - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites History Print Copy Paste Refresh Stop Links

Address C:\TechDocs\IIS Security\IISLock\Tool\DataEntry\Default.htm Go Links >>

Windows 2000 Internet Server Security Configuration Tool

- Home
- View the [README file](#)
- Build a [Security Template](#)
- [Microsoft Security Web Site](#)
- [About and Legal Notice](#)

Build a Security Template

I wish to:

- Remotely administer this computer using Windows Networking.
- Remotely administer this computer over the Web.
- Use this server as a File Transfer Protocol server (FTP)
- Use this server as an Internet email server (SMTP, POP3)
- Use this computer as an Internet news (NNTP) server
- Use Secure Sockets Layer/Transport Layer Security (SSL/TLS) on this server
- Use this computer as Telnet server
- Allow files other than static files (.txt, .html, .gif etc) and Active Server Pages to be served.
 - Use Internet Printing
 - Use Server Side Includes (SSI)
 - Change Windows passwords over the Web
 - Use Index Server with IIS
- Keep the Web samples

Template Name:

Done My Computer

IIS Security Configuration Tool (cont'd)

- Deployment phase

- Use the IISConfig command line tool to deploy the IISTemplate.txt file

- Usage: IISConfig [-s server] [-f configfile] [-n] [-d] [-? | -h]

- Where:

<code>[-s server]</code>	is the server name (DNS or NetBIOS; IP address is not supported)
<code>[-f configfile]</code>	is the configuration file name
<code>[-n]</code>	configures port lockdown, services and IIS script maps only. Does not use SCE hisecweb.inf
<code>[-d]</code>	display debug output as tool executes
<code>[-?]</code>	display help

IIS Security Configuration Tool (cont'd)

- Subdirectories
 - DataEntry directory
 - Where you enter your security policy
 - Engine directory
 - Where script files used to deploy policy are stored
- More information
 - Read the ReadMe.txt file for more information and known issues

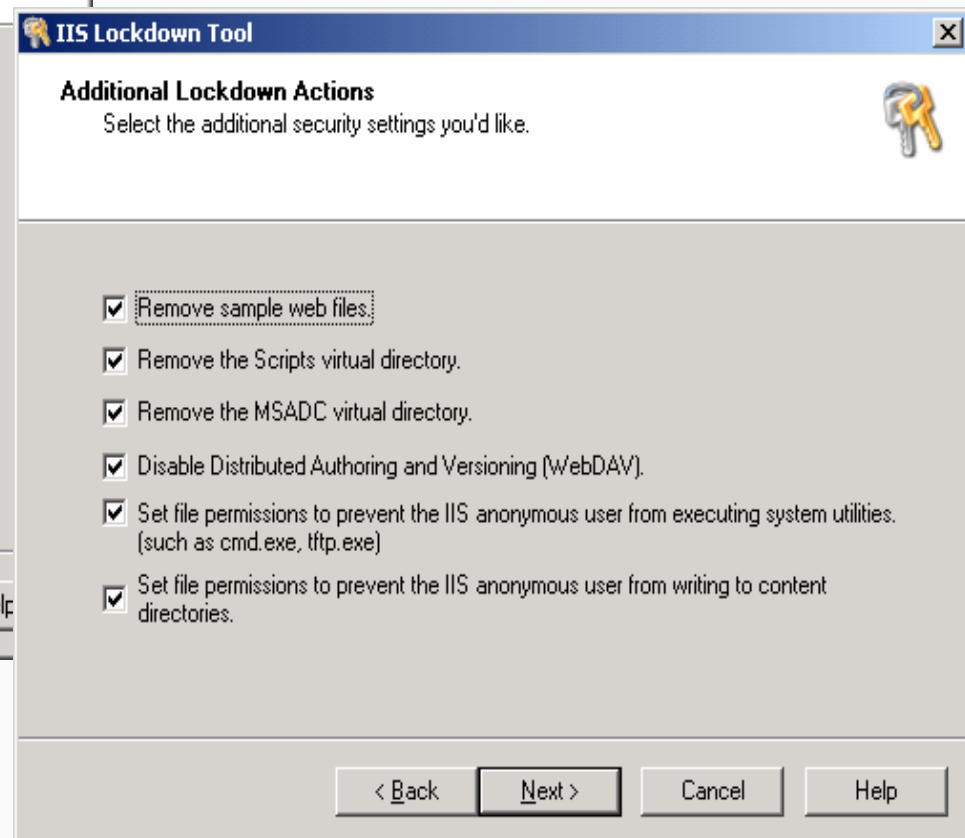
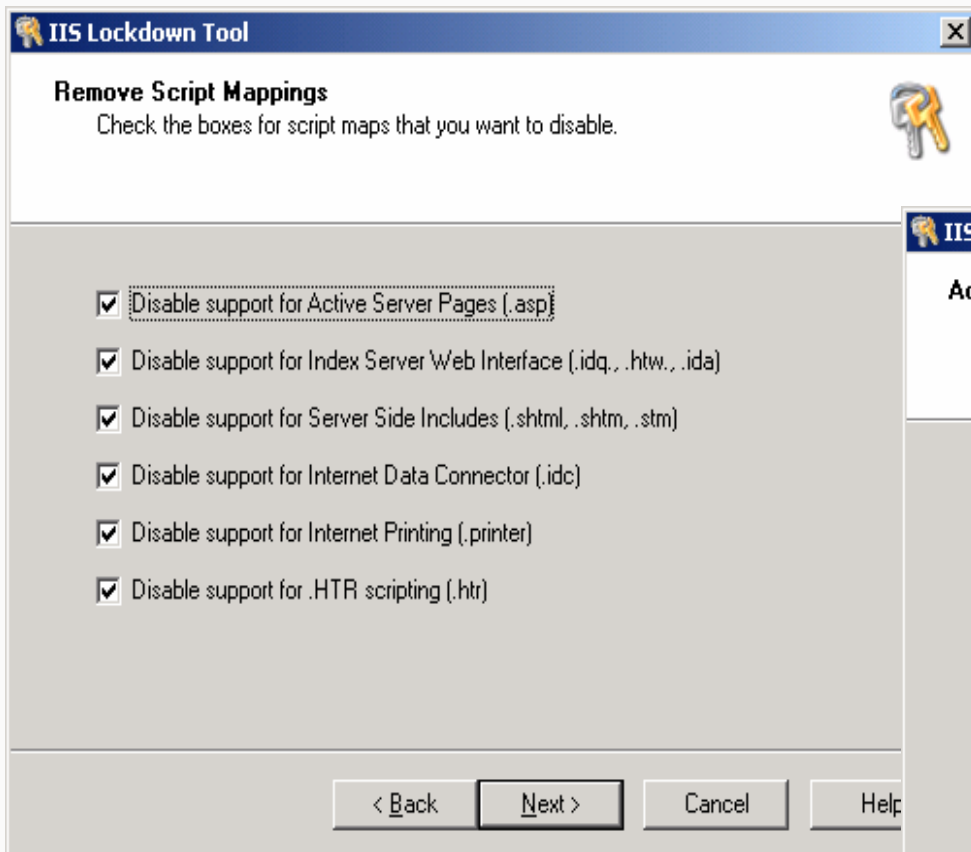
Lockdown

Lockdown

- Disable:
 - ASP Pages
 - Index Server Pages
 - Server Side Includes
 - IDC Database Connector
 - Internet Printing
 - .HTR Scripting
 - /MSADC Virtual Folder
 - WebDAV
- ◆ Removes IIS Samples
- ◆ Sets NTFS Permissions

IIS Lockdown Tool

Advanced Lockdown Settings Screenshots



URLScan

- ISAPI Filter
- Analyze and screen HTTP request
- Reduces exposure to potential attacks
- Allows configuration of IIS to reject requests based on the following criteria:
 - The request method (verb)
 - The file extension of the resource requested
 - Suspicious URL encoding
 - Presence of non ASCII characters in the URL
 - Presence of particular character sequences in the URL
 - Presence of particular headers in the request
- Also provides the option of deleting or altering the “Server:” header in the response

URLScan Configuration

- UrlScan's operation is controlled by the UrlScan.ini file
- UrlScan.ini should reside in the same directory as UrlScan.dll
- Note that UrlScan only reads the ini file at initialization time (for performance reasons)
 - It is necessary to stop and start the web service before any changes to this file will be effective
- Also note that the default options built into UrlScan.dll will result in a configuration that will reject all requests to the server.
 - It is necessary to provide a UrlScan.ini file for UrlScan to pass requests to be served
 - A sample UrlScan.ini file is provided that contains the recommended settings to defend against known attacks against IIS servers at the time of writing

URLScan Logging

- If a request is denied, the following will be logged
 - Reason for the denial
 - Information about the request
 - Typically, the URL and IP address of the source of the request

URLScan Logfile Screenshot

```
UrlScan.log - Notepad
File Edit Format Help
[Wed, Aug 29 2001 - 12:55:37] ----- UrlScan.dll initializing -----
[Wed, Aug 29 2001 - 12:55:37] URLs will be normalized before analysis.
[Wed, Aug 29 2001 - 12:55:37] URL normalization will be verified.
[Wed, Aug 29 2001 - 12:55:37] URLs may contain OEM, international and UTF-8 characters.
[Wed, Aug 29 2001 - 12:55:37] URLs must not contain any dot except for the file extension.
[Wed, Aug 29 2001 - 12:55:37] Only the following verbs will be allowed (case sensitive):
[Wed, Aug 29 2001 - 12:55:37] 'GET'
[Wed, Aug 29 2001 - 12:55:37] 'HEAD'
[Wed, Aug 29 2001 - 12:55:37] 'POST'
[Wed, Aug 29 2001 - 12:55:37] Requests for following extensions will be rejected:
[Wed, Aug 29 2001 - 12:55:37] '.exe'
[Wed, Aug 29 2001 - 12:55:37] '.bat'
[Wed, Aug 29 2001 - 12:55:37] '.cmd'
[Wed, Aug 29 2001 - 12:55:37] '.com'
[Wed, Aug 29 2001 - 12:55:37] '.htw'
[Wed, Aug 29 2001 - 12:55:37] '.ida'
[Wed, Aug 29 2001 - 12:55:37] '.idq'
[Wed, Aug 29 2001 - 12:55:37] '.htr'
[Wed, Aug 29 2001 - 12:55:37] '.idc'
[Wed, Aug 29 2001 - 12:55:37] '.shtm'
[Wed, Aug 29 2001 - 12:55:37] '.shtml'
[Wed, Aug 29 2001 - 12:55:37] '.stm'
[Wed, Aug 29 2001 - 12:55:37] '.printer'
[Wed, Aug 29 2001 - 12:55:37] '.ini'
[Wed, Aug 29 2001 - 12:55:37] '.log'
[Wed, Aug 29 2001 - 12:55:37] '.pol'
[Wed, Aug 29 2001 - 12:55:37] '.dat'
[Wed, Aug 29 2001 - 12:55:37] Requests containing the following headers will be rejected:
[Wed, Aug 29 2001 - 12:55:37] 'translate:'
[Wed, Aug 29 2001 - 12:55:37] 'if:'
[Wed, Aug 29 2001 - 12:55:37] 'lock-token:'
[Wed, Aug 29 2001 - 12:55:37] Requests containing the following character sequences will be
rejected:
[Wed, Aug 29 2001 - 12:55:37] '..'
[Wed, Aug 29 2001 - 12:55:37] './'
[Wed, Aug 29 2001 - 12:55:37] '\'
[Wed, Aug 29 2001 - 12:55:37] ':'
[Wed, Aug 29 2001 - 12:55:37] '%'
[Wed, Aug 29 2001 - 12:55:37] '&
```

If You Got Hacked...

- Have a “Incident Response Plan”
- Remove machines from the net
- Find out how the hacker did it
- Perform a low-level format
- Examine connected computers

Resources

- Microsoft Security
 - <http://www.microsoft.com/security>
 - Technet-IIS Checklists 5.0
[http://www.microsoft.com/technet/treeview/default.asp?url= /technet/prodtechnol/iis/tips/iis5chk.asp](http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/iis/tips/iis5chk.asp)
- SANS
 - <http://www.sans.org/>
- NSA Security Recommendations
 - <http://nsa2.www.conxion.com/win2k/guides/w2k-14.pdf>
- National Strategy for Securing Cyberspace
 - <http://www.whitehouse.gov/pcipb/cyberstrategy-draft.pdf>



Questions ?

Thank You

bhupendra@cert-in.org.in

<http://www.cert-in.org.in>