Securing IIS Servers

Presented to WNUG
Nov. 1, 2001
By
Mehran Yahya & Pat Schneider

Securing IIS Servers

- Installation
- Authentication
- Permissions and Authorization
- Web Applications
- Protect the Metabase
- Monitoring and Logging
- Utilities
- Miscellaneous
- Web sites, products, training

Securing IIS Servers

- Installation
  - Only install necessary components
  - Do not have server connected to ethernet during the installation
  - Apply all service packs and hot fixes
  - Remove printer and file support
  - Disable unnecessary services and subsystems

Securing IIS Server

- DHCP Client
- DFS
- Fax Service
- FTP Publishing
- Indexing Service
- NNTP
- Print Spooler
- NNTP Service
- IPSec Policy Agent
- RunAs
- Smart Card
- Smart Card Helper
- Telephony
- Telnet
- Terminal Services
- WMI
- WMI Driver Extensions
- NetMeeting
- Messenger
- SMTP Service

Securing IIS Servers

- Installation (cont.)
  - Delete sample files
  - Delete or move sample scripts
  - Remove Internet Explorer
  - Security Templates
  - Remove any resource kits or SDKs that were installed
  - Secure dangerous executables

Securing IIS Servers

- ARP.EXE
- AT.EXE
- ATTRIB.EXE
- CMD.EXE
- COMMAND.EXE
- CSCRIPT.EXE
- FTP.EXE
- NET.EXE
- NET1.EXE
- TFTP.EXE
- WSCRIPT.EXE
- HYPERTERM.EXE
- HTIMAGE.EXE
- IPCONFIG.EXE
- NBSTAT.EXE
- PING.EXE
- POLEDIT.EXE
- QBASIC.EXE
- REGEDIT.EXE
- REGEDIT32.EXE
- RUNAS.EXE
- XCOPY.EXE

Securing IIS Servers

- Authentication
  - Anonymous access
  - Use of SSL

Securing IIS Servers

- Permissions & Authorization
  - NTFS permissions for website content volumes
    - Set initial NTFS permissions settings on the root of the volume
      - Administrators: Full control (Apply onto: This folder, subfolders, and files)
      - System: Full control (Apply onto: This folder, subfolders and files)
      - Check the box on the Permissions tab to "Reset permissions on all child objects and enable propagation of inheritable permissions"

Securing IIS Servers

- Permissions & Authorization
  - NTFS permissions for website content volumes
    - Set initial NTFS audit settings on the root of the volume
      - Everyone: Failed
      - Everyone: Successful
        - Create File/Append Data
        - Create Folders/Append Data
        - Delete Subfolders and Files
        - Delete
        - Change Permissions
        - Take Ownership
      - Check the box on the Auditing tab to "Reset auditing entries on all child objects and enable propagation of inheritable auditing entries"

Securing IIS Servers

- Permissions & Authorization
  - NTFS permissions for IIS files
    - Anonymous access – Read only
    - System, Administrators & Operators – Full Control
    - Authors – Modify (includes all permissions as Full Control except Take Ownership, Change Permissions, and Delete Subfolders and Files)
    - Individual Groups – Whatever permissions are necessary for the roles determined for the groups

Securing IIS Servers

- Permissions & Authorization
  - IIS Permissions
    - Four IIS permissions for the contents of folders; control what HTTP commands the server will accept from the browser
      - Read
      - Write
      - Script Source Access
      - Directory Browsing
    - Three application permissions (Execute)
      - None
      - Scripts Only
      - Scripts and Executables

Securing IIS Servers

- Permissions & Authorization
  - Best Practices for Website Folders
    - Physical folder structure
      - /root – starting point of the website
        - Home page
      - /scr – stores scripts
        - Don't call it "scripts" as this is a tip-off for hackers
      - /exe – executables
        - Don't call it "bin" or "cgi-bin" as this is a tip-off for hackers; may not even want to call it "exe"
      - /images – graphics
        - Reduces clutter in other folders and can be removed from logging

Securing IIS Servers

- Permissions & Authorization
  - Best Practices for Website Folders
    - Write IIS permission should not be assigned to any folder unless that folder has been specially created and secured for content authors.
    - Write and Execute IIS permissions should never be assigned to any folder accessible to anonymous users.
    - Script Source Access IIS permission should not be assigned to any folder unless that folder has been specially created and secured for content authors.
    - No folder should have more IIS or NTFS permissions than necessary to allow legitimate browsing and authoring by the appropriate groups.
    - Do not enable Directory Browsing IIS permission on a folder unless you specifically want anonymous users to see every file and subfolder.
    - Avoid using folder names that are obvious as this makes them vulnerable to attacks.

Securing IIS Servers

- Web Applications
  - ISAPI Filters vs ISAPI Extensions
    - Filters are DLLs which register "hooks" with IIS so that they will be invoked when certain internal IIS events occur.
      - Event triggers pass control of a request or response to an ISAPI filter DLL (Example: SSL encryptions)
    - Extensions are DLLs or programs which are associated with files of a certain filename extensions so that when a browser makes a request to such a file, the program is automatically executed.
      - Typically script engines or command interpreters

Securing IIS Servers

- Unmap Unused ISAPI Extensions and HTTP Verbs
  - Map .HTM files to the ASP.DLL
    - Conceal the fact that you are using Active Server Pages by associating .htm files with ASP.DLL and leave .html files as regular static pages
  - Remove unused HTTP verbs
    - Most pages usually only need GET and POST
  - Mappings will reappear any time you change a Windows Component using Add/Remove Programs in the Control Panel
    - ADSUTIL.VBS script installed with IIS can be used to show or set values in the metabase

Securing IIS Servers

- ISAPI Filters
  - Four default filters
    - SSPIFILT.DLL – implements SSL encryption for all websites using HTTPS
    - COMPFILT.DLL – implements HTTP compressions of requested files using GZIP and DEFLATE protocols
    - MD5FILT.DLL – used with Digest authentication
    - FPEXEDLL.DLL – provides compatibility with FrontPage

Securing IIS Servers

- Delete Unused ISAPI Filters
  - All ISAPI filters are loaded into the process space INETINFO.EXE and run with System context.
  - Remove filters in both the Master-Level property sheet for the WWW Service and in the property sheet of each website.
    - Remove FPEXEDLL.DLL if you're not using FrontPage
    - Remove MD5FILT.DLL if you're not using Digest authentication
    - Remove SSPIFILT.DLL if you're not using SSL encryption or certificate authentication
    - Remove COMPFILT.DLL to disable HTTP compression if security is more important than performance.

Securing IIS Servers

- Protect the Metabase
  - The "metabase" is IIS's configuration database (like the system registry)
    - Location is determined by a registry value which can be modified (not recommended unless you're paranoid!)
      - **Hive:** **HKEY_LOCAL_MACHINE**
      - **Key:** **\Software\Microsoft\InetMgr\Parameters**
      - **Value Name:** **MetadataFile**
      - **Value Type:** **REG_SZ**
      - **Value Data:** **<drive letter, path, and filename of the metabase>**

Securing IIS Servers

- Protect the Metabase (cont.)
  - Move the HTTP/FTP root folders off the %systemroot% volume
  - Secure the registry key which determines the metabase location
  - Audit all failed access to the metabase file
  - Set NTFS permissions on the metabase file to the following:
    - Administrators: Full Control
    - System: Full Control

Securing IIS Servers

- Protect the Metabase (cont.)
  - After configuring IIS, backup the metabase
    - Use the "official" backup method using the IIS snap-in
      - Right-click the computer, select Action, Backup/Restore Configuration, Create Backup
    - Secure the default backup file
      - %systemroot%\System32\Inetsrv\MetaBack.MDO

Securing IIS Servers

- Monitoring and Logging
  - Use performance monitor
    - Log monitor output to a data file
    - Determine an appropriate period of time for monitoring activity
    - Get a baseline set of statistics

Securing IIS Servers

- What to Monitor?
  - Active Server Pages
    - Errors/Sec
    - Request Not Authorized
  - Disk
    - Logical Disk\% of Free Space
  - IP
    - Datagrams Received Header Errors
    - Datagrams Received Unknown Protocol
    - Fragment Re-Assembly Failures

Securing IIS Servers

- What to Monitor? (cont.)
  - Memory
    - Available Mbytes
  - Network Interface
    - Packets Received Errors
    - Packets Received Unknown
  - Paging File
    - % Usage
  - Processor
    - % Processor Time

Securing IIS Servers

- What to Monitor? (cont.)
  - Server
    - Errors Access Permissions
    - Errors Granted Access
    - Errors Logon
  - TCP
    - Connection Failures
    - Connections Reset
  - UDP
    - Datagrams No Port/Sec

Securing IIS Servers

- What to Monitor? (cont.)
  - Web Service
    - Anonymous Users/Sec
    - NonAnonymous User/Sec
    - Connection Attempts/Sec
    - Logon Attempts/Sec
    - Not Found Errors/Sec
    - Other Request Methods/Sec
    - Service Uptime

Securing IIS Servers

- Event Viewer Logs
  - Enable Auditing
    - Account Logon Events: Success, Failure
    - Account Management: Success, Failure
    - Directory Service Access: Failure
    - Logon Events: Success, Failure
    - Object Access: Success, Failure
    - Policy Change: Success, Failure
    - Privilege Use: Success, Failure
    - Process Tracking: None
    - System Events: None

Securing IIS Servers

- Event Viewer Logs
  - NTFS File Access Audit
    - Audit all the different types of failed access for the entire file system
    - Audit successful actions for Everyone for:
      - Create Files / Write Data
      - Create Folder / Append Data
      - Delete Subfolders and Files
      - Delete
      - Change Permissions
      - Take Ownership

Securing IIS Servers

- IIS Protocol Logging
  - Enable logging at the website
  - Disable logging for each folder/file you don't want to log
  - Set the location for the log files
  - Secure the log files using NTFS permissions

Securing IIS Servers

- Date
- Time
- Client IP Address
- User Name
- Method
- URI System
- URI Query
- Protocol Status
- Win32 Status
- Service Name
- Service Name
- Server IP
- Server Port
- Bytes Sent
- Bytes Retrieved
- Time Taken
- Protocol Version
- Host
- User Agent
- Cookie
- Referrer

Securing IIS Servers

- Utilities
  - Resource Kit
    - METAEDIT.EXE – IIS configuration tool
    - PLAYBACK.EXE – Records incoming traffic on an IIS 5.0 server then allows it to be played back on another server
    - Stress test utility
    - IIS Permissions Wizard Template Maker

Securing IIS Servers

- Utilities (cont.)
  - Command Line
    - ADSUTIL.VBS – Metabase configuration
    - IISRESET.EXE – stop/start IIS services; reboot the server
    - SECEDIT.EXE – Applies security templates
    - HFNETCHK.EXE – Network security hotfix checker
    - QCHAIN.EXE – Installs multiple hotfixes
    - QFECHECK.EXE – Verifies successful installation of hotfixes
    - SFC.EXE – Windows file protection; checks for corrupt system files
    - NETSTAT.EXE – many uses; one to determine if system is being SYN-flooded

Securing IIS Servers

- Miscellaneous
  - Throttling IIS
    - Limit connections
    - Set connection timeouts
  - Administration Website (HTMLA)
    - Secure the site with SSL, authentication, IP address restrictions

Securing IIS Servers

- Miscellaneous
  - FrontPage
    - Keep current with updates
    - Require SSL and IP filtering when authoring
    - See the chapter in the FrontPage Resource Kit on security (Online version can be found at http://www.microsoft.com/frontpage/wpp/SERK)
    - Refer to TechNet for additional FrontPage security topics

Securing IIS Servers

- References – Web Sites
  - Microsoft Sites
    - http://microsoft.com/security
    - http://microsoft.com/technet/iis
    - http://microsoft.com/technet/iis/frontpg.asp
    - http://webtool.rte.microsoft.com

Securing IIS Servers

- References – Web Sites (cont.)
  - Other Sites
    - http://packetstormsecurity.com
    - http://www.securityfocus.com
    - http://nsa1.www.conxion.com
    - http://www.15seconds.com/focus/Security.htm
    - http://staff.washington.edu/dittrich/misc/ddos
    - http://www.insecure.org/nmap
    - http://www.ietf.org
    - http://www.iisfaq.com

Securing IIS Servers

- References – E-Mail Bulletins
  - http://www.sans.org
  - http://www.microsoft.com/security
  - http://www.securityfocus.com
  - http://www.ntshop.net

Securing IIS Servers

- References – Books & Magazines
  - *Windows 2000 Magazine*
    - http://www.win2000mag.com
  - *Designing Secure Web-Based Applications for Microsoft Windows 2000* by M. Howard, M. Levy and R. Waymire (Microsoft Press)
  - *Hacking Exposed Windows 2000* by Joel Scambray, Stuart McClure (McGraw-Hill)
  - *Securing Windows NT/2000 Servers for the Internet* by Stefan Norberg, Deborah Russell (O'Reilly)
  - *Windows 2000 Security* by Roberta Bragg (New Riders)

Securing IIS Servers

- References – Third Party Products
  - ISS

Securing IIS Servers

- References – Training
  - SANS Institute
    - Securing Internet Information Server 5.0
      - This course is available as a classroom course or online
      - http://www.sans.org