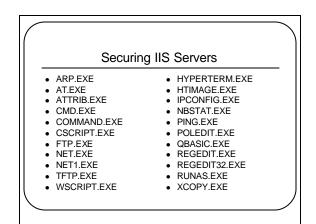
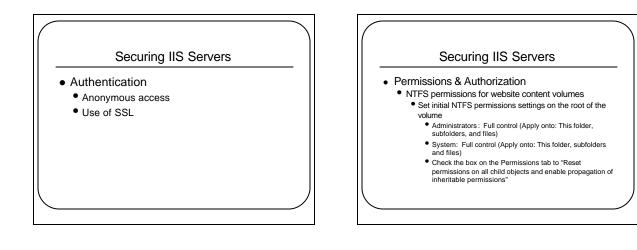


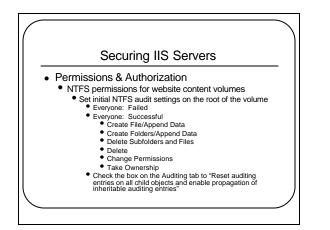
- Smart Card •
 - Smart Card Helper
 - Telephony
 - Telnet
 - Terminal Services
- WMI
- WMI Driver Extensions
 - NetMeeting
 - Messenger
 - SMTP Service

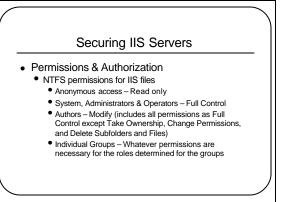
Securing IIS Servers

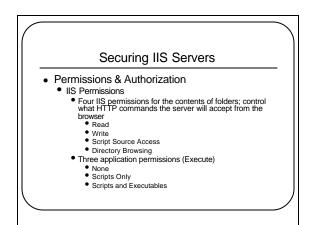
- Installation (cont.)
 - Delete sample files
 - Delete or move sample scripts
 - Remove Internet Explorer
 - Security Templates
 - Remove any resource kits or SDKs that were installed
 - Secure dangerous executables

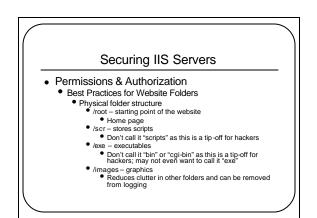












Securing IIS Servers

- Permissions & Authorization Best Practices for Website Folders
 - Write IIS permission should not be assigned to any folder unless that folde has been specially created and secured for content authors.

 - has been spectary ureared and secured for content admons. 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: unless t authors
 - No folder should have more IIS or NTFS permissions than necessary to

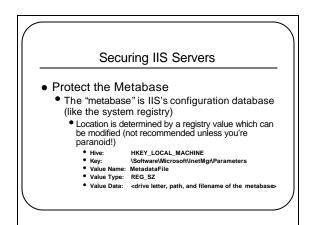
 - Do not enable Directory Browsing and authoring by the appropriate groups.
 Do not enable Directory Browsing IIS permission on a folder unless you specifically want anonymous users to see every file and subfolder.
 - Avoid using folder names that are obvious as this makes them vulnerable to attacks.

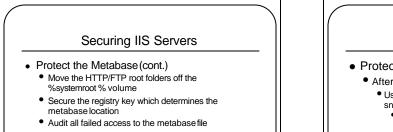
Securing IIS Servers Web Applications ISAPI Filters vs ISAPI Extensions Filters are DLLs which register "hooks" with IIS so that they will be invoked when certain internal IIS events occur. Event triggers pass control of a request or response to an ISAPI filter DLL (Example: SSL encryptions) • Extensions 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

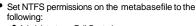
Securing IIS Servers Unmap Unused ISAPI Extensions and HTTP Verbs Map .HTM files to the ASP.DLL Conceal the fact that you are using Active Server Pages by associating .htm files with ASP.DLL and leave .html files as regular static pages Remove unused HTTP verbs Most pages usually only need GET and POST 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

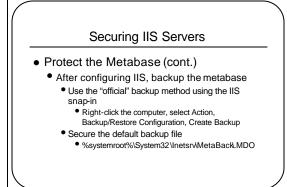
Securing IIS Servers **Delete Unused ISAPI Filters** All ISAPI filters are loaded into the process space INETINFO.EXE and run with System context. Remove filters in both the Master-Level property sheet for the WWW Service and in the property sheet of each website. Remove FPEXEDLL.DLL if you're not using 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.

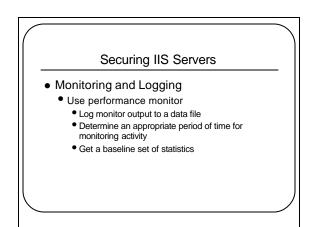


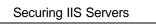




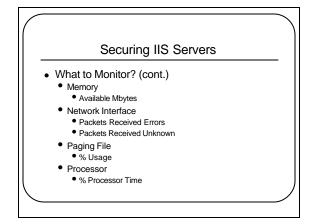
- Administrators: Full Control
- System: Full Control

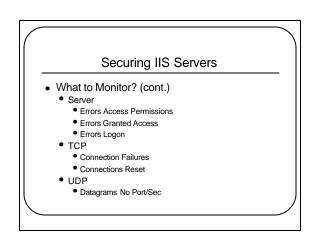






- What to Monitor?
 - Active Server Pages
 - Errors/Sec
 - Request Not Authorized
 - Disk
 - Logical Disk\% of Free Space
 - IP
 - Datagrams Received Header Errors
 - Datagrams Received Unknown Protocol
 - Fragment Re-Assembly Failures

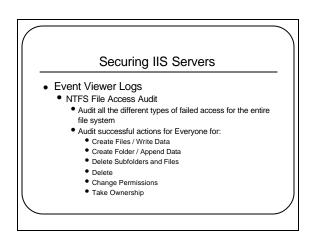


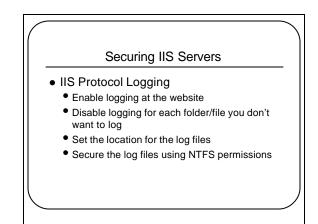


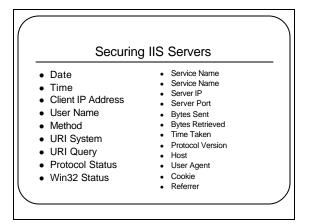
Securing IIS Servers What to Monitor? (cont.) Web Service Anonymous Users/Sec NonAnonymous User/Sec Connection Attempts/Sec

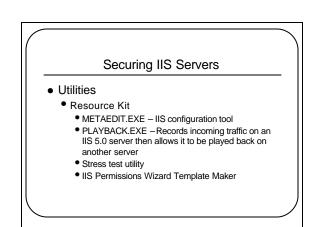
- Logon Attempts/Sec
- Not Found Errors/Sec
- Other Request Methods/Sec
- Service Uptime

Securing IIS Servers • Event Viewer Logs • Enable Auditing • Account Logon Events: Success, Failure • Account Management: Success, Failure • 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 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
 - <u>http://microsoft.com/security</u>
 - 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 • <u>http://www.sans.org</u> • <u>http://www.microsoft.com/security</u> • <u>http://www.securityfocus.com</u> • <u>http://www.ntshop.net</u>

Securing IIS Servers • References – Books & Magazines • Windows 2000 Magazine • http://www.win2000magazine • http://www.win2000magazine • Designing Secure Web-Based Applications for Microsoft Windows 2000 by M. Howard, M. Levy and R. Waymire (Microsoft Press) • Hacking Exposed Windows 2000by 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

