Windows IIS server hardening checklist

General

- ☐ Never connect an IIS server to the internet until it is fully hardened.
- ☐ Place the server in a physically secure location.
- ☐ Do not install the IIS server on a domain controller.
- ☐ Do not install a printer.
- ☐ Use two network interfaces in the server: one for admin and one for the network.
- ☐ Install service packs, patches and hot fixes.
- ☐ Run Microsoft Security Compliance Toolkit.
- ☐ Run IIS Lockdown on the server.
- ☐ Install and configure URLScan.
- ☐ Secure remote administration of the server, and configure for encryption, low session timeouts and account lockouts.
- ☐ Disable unnecessary Windows services.
- ☐ Ensure services are running with least-privileged accounts.
- ☐ Disable FTP, Simple Mail Transfer Protocol and Network News Transfer Protocol services if they are not required.
- ☐ Disable Telnet service.
- ☐ Disable ASP.NET state service if not used by your applications.
- ☐ Disable Web Distributed Authoring and Versioning if not used by the application, or secure it if it is required.
- ☐ Do not install Microsoft Data Access Components (MDAC) unless specifically needed.
- ☐ Do not install the HTML version of Internet Services Manager.
- ☐ Do not install Microsoft Index Server unless required.
- ☐ Do not install Microsoft FrontPage Server Extensions (FPSE) unless required.
- ☐ Harden the TCP/IP stack.
- ☐ Disable NetBIOS and Server Message Block—closing ports 137, 138, 139 and 445.
- ☐ Reconfigure recycle bin and page file system data policies.
- ☐ Secure CMOS (complementary metal-oxide semiconductor) settings.
- ☐ Secure physical media—CD-ROM drive and so on.

Accounts

- ☐ Remove unused accounts from the server.
- ☐ Disable Windows Guest account.
- ☐ Rename Administrator account, and set a strong password.
- ☐ Disable IUSR_Machine account if it is not used by the application.
- ☐ Create a custom least-privileged anonymous account if applications require anonymous access.
- ☐ Do not give the anonymous account write access to web content directories or allow it to execute command-line tools.
- ☐ If you host multiple web applications, configure a separate anonymous user account for each one.

©2020 TECHTARGET. ALL RIGHTS RESERVED TechTarget

- ☐ Configure ASP.NET process account for least privilege. This only applies if you are not using the default ASP.NET account, which is a least-privileged account.
- ☐ Enforce strong account and password policies for the server.
- ☐ Enforce two-factor authentication where possible.
- ☐ Restrict remote logons. (The "access this computer from the network" user right is removed from the Everyone group.)
- ☐ Do not share accounts among administrators.
- ☐ Disable null sessions (anonymous logons).
- ☐ Require approval for account delegation.
- ☐ Do not allow users and administrators to share accounts.
- ☐ Do not create more than two accounts in the administrator group.
- ☐ Require administrators to log on locally, or secure the remote administration system.

Files and directories

- ☐ Use multiple disks or partition volumes, and do not install the web server home directory on the same volume as the OS folders.
- ☐ Contain files and directories on NT file system (NTFS) volumes.
- ☐ Put website content on a nonsystem NTFS volume.
- ☐ Create a new site, and disable the default site.
- ☐ Put log files on a nonsystem NTFS volume but not on the same volume where the website content resides.
- ☐ Restrict the Everyone group—no access to \WINNT\system32 or web directories.
- ☐ Ensure website root directory has deny write access control entry (ACE) for anonymous internet accounts.
- ☐ Ensure content directories have deny write ACE for anonymous internet accounts.
- ☐ Remove resource kit tools, utilities and SDKs.
- ☐ Remove any sample applications or code.
- ☐ Remove IP address in header for Content-Location.

Shares

- ☐ Remove all unnecessary shares, including default administration shares.
- ☐ Restrict access to required shares—the Everyone group does not have access.
- ☐ Remove administrative shares—C$ and Admin$ -- if they are not required. (Microsoft System Center Operations Manager—formerly Microsoft Systems Management Server and Microsoft Operations Manager—requires these shares.)

Ports

- ☐ Restrict internet-facing interfaces to port 443 (SSL).
- ☐ Run IIS Lockdown Wizard on the server.

Registry

- ☐ Restrict remote registry access.
- ☐ Secure the local Security Account Manager (SAM) database by implementing the NoLMHash Policy.

Auditing and logging

- ☐ Audit failed logon attempts.
- ☐ Relocate and secure IIS log files.
- ☐ Configure log files with an appropriate file size depending on the application security requirement.
- ☐ Regularly archive and analyze log files.
- ☐ Audit access to the MetaBase.xml and MBSchema.xml files.
- ☐ Configure IIS for World Wide Web Consortium extended log file format auditing.
- ☐ Read how to use SQL Server to analyze web logs here.

Sites and virtual directories

- ☐ Put websites on a nonsystem partition.
- ☐ Disable Parent Paths setting.
- ☐ Remove any unnecessary virtual directories.

©2020 TECHTARGET. ALL RIGHTS RESERVED TechTarget

- ☐ Remove or secure MDAC Remote Data Services virtual directory.
- ☐ Do not grant included directories read web permission.
- ☐ Restrict write and execute web permissions for anonymous accounts in virtual directories.
- ☐ Ensure there is script source access only on folders that support content authoring.
- ☐ Ensure there is write access only on folders that support content authoring and these folders are configured for authentication and SSL encryption.
- ☐ Remove FPSE if not used. If FPSE are used, update and restrict access to them.
- ☐ Remove the IIS Internet Printing virtual directory.

Script mappings

- ☐ Map extensions not used by the application to 404.dll—.idq, .htw, .ida, .shtml, .shtm, .stm, idc, .htr, .printer.
- ☐ Map unnecessary ASP.NET file type extensions to HttpForbiddenHandler in Machine.config.

ISAPI filters

- ☐ Remove unnecessary or unused Internet Server Application Program Interface filters from the server.

IIS Metabase

- ☐ Restrict access to the metabase by using NTFS permissions (%systemroot%\system32\inetsrv\metabase.bin).
- ☐ Restrict IIS banner information (disable IP address in content location).

Server certificates

- ☐ Ensure certificate date ranges are valid.
- ☐ Only use certificates for their intended purpose. For example, the server certificate is not used for email.
- ☐ Ensure the certificate's public key is valid, all the way to a trusted root authority.
- ☐ Confirm that the certificate has not been revoked.

Machine.config

- ☐ Map protected resources to HttpForbiddenHandler.
- ☐ Remove unused HttpModules.
- ☐ Disable tracing: <trace enable=" false"/>.
- ☐ Turn off debug compiles: <compilation debug="false" explicit="true" default Language="vb">.

©2020 TECHTARGET. ALL RIGHTS RESERVED TechTarget