Windows IIS Server hardening checklist

By Michael Cobb

General

- Do not 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 IISLockdown run on the server.
- Install and configure URLScan.
- Secure remote administration of the server and configure for encryption, low session time-outs and account lockouts.
- Disable unnecessary Windows services.
- Ensure services are running with least-privileged accounts.
- Disable FTP, SMTP and NNTP services if they are not required.
- Disable Telnet service.
- Disable ASP.NET state service if not used by your applications.
- Disable webDAV if not used by the application, or secure it if it is required. (See How To: Create a secure webDAV Publishing Directory at support.microsoft.com.)

- Do not install Data Access Components unless specifically needed.
- Do not install the HTML version of the Internet Services Manager.
- Do not install the MS Index Server unless required.
- Do not install the MS FrontPage Server extensions unless required.
- Harden TCP/IP stack.
- Disable NetBIOS and SMB (closing ports 137, 138, 139 and 445).
- Reconfigure Recycle Bin and Page file system data policies.
- Secure CMOS settings.
- Secure physical media (floppy drive, 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.
- 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.
- 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 Administrators group.
- Require administrators to log on locally or secure the remote administration solution.

Files and Directories

- Use multiple disks or partition volumes and do not install the Web server home directory on the same volume as the operating system folders.
- Contain files and directories on NTFS volumes.
- Put Web site content on a non-system NTFS volume.
- Create a new site and disable the default site.
- Put log files on a non-system NTFS volume but not on the same volume where the Web site content resides.
- Restrict the Everyone group (no access to \WINNT\system32 or Web directories).
- Ensure Web site root directory has deny write ACE for anonymous Internet accounts.
- Ensure content directories have deny write ACE for anonymous Internet accounts.
- Remove remote IIS administration application (\WINNT\System32\Inetsrv\IISAdmin).

- Remove resource kit tools, utilities and SDKs.
- Remove sample applications (\WINNT\Help\IISHelp, \Inetpub\IISSamples).
- 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 Management Server (SMS) and Microsoft Operations Manager (MOM) require these shares).

Ports

- Restrict Internet-facing interfaces to port 80 (and 443 if SSL is used).
- Encrypt Intranet traffic (for example, with SSL), or restrict Internet traffic if you do not have a secure data center infrastructure.

Registry

- Restrict remote registry access.
- Secure SAM (HKLM\System\CurrentControlSet\Control\LSA\NoLMHash). This applies only to standalone servers.

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.bin file.
- Configure IIS for W3C Extended log file format auditing.
- Read How to use SQL Server to analyze Web logs at support.microsoft.com

Sites and Virtual Directories

- Put Web sites on a non-system partition.
- Disable "Parent paths" setting.
- Remove potentially dangerous virtual directories including IISSamples, IISAdmin, IISHelp and Scripts.
- Remove or secure MSADC virtual directory (RDS).
- 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, if required).
- Remove FrontPage Server Extensions (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 from the server unnecessary or unused ISAPI filters.

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 e-mail).
- 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" defaultLanguage="vb">
```