Server Hardening Checklist

Introduction

The following checklist can be used to identify the elements a vendor recommends as viable and substantial items for server hardening. Select a subset of these items to forward to clients and their technical support personnel to obtain server hardening conformance.

Other server checklists are accessed via URLs at the end of this document. Compile an appropriate list from all information for each validated offering. The final document is ultimately a guide which can be included with other guidelines for a vendor sanctioned server hardening routines.

Windows IIS Server hardening checklist

1. **General**
    a. Do not connect a Server to the Internet until it is fully hardened.
    b. Place the server in a physically secure location.
    c. Do not install the IIS server on a domain controller.
    d. Do not install a printer.
    e. Use two network interfaces in the server — one for admin and one for the network.
    f. Install service packs, patches and hot fixes.
    g. Run IISLockdown run on the server.
    h. Install and configure URLScan.
    i. Secure remote administration of the server and configure for encryption, low session time-outs and account lockouts.
    j. Disable unnecessary Windows services. List services.
    k. Ensure services are running with least-privileged accounts.
    l. Disable FTP, SMTP and NNTP services if they are not required.
    m. Disable Telnet service.
    n. Disable ASP.NET state service if not used by your applications.
    o. Disable webDAV if not used by the application, or secure it if it is required. (See
    p. How To: Create a secure webDAV Publishing Directory at support.microsoft.com.)
    q. Do not install Data Access Components unless specifically needed.
    r. Do not install the HTML version of the Internet Services Manager.
    s. Do not install the MS Index Server unless required.
    t. Do not install the MS FrontPage Server extensions unless required.
    u. Harden TCP/IP stack.
    v. Disable NetBIOS and SMB (closing ports 137, 138, 139 and 445).
    w. Reconfigure Recycle Bin and Page file system data policies.
    x. Secure CMOS settings.
    y. Secure physical media (floppy drive, CD-ROM drive and so on).

2. **Accounts**
    a. Remove unused accounts from the server.
    b. Disable Windows Guest account.
    c. Rename Administrator account and set a strong password.
    d. Disable IUSR_MACHINE account if it is not used by the application.
    e. Create a custom least-privileged anonymous account if applications require anonymous access.
    f. Do not give the anonymous account write access to Web content directories or allow it to execute command-line tools.
    g. If you host multiple Web applications, configure a separate anonymous user account for each one.
    h. 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.)
    i. Enforce strong account and password policies for the server.
    j. Restrict remote logons. (The "Access this computer from the network" user-right is removed from the Everyone group.)
    k. Do not share accounts among administrators.
    l. Disable Null sessions (anonymous logons).
    m. Require approval for account delegation.
    n. Do not allow users and administrators to share accounts.
    o. Do not create more than two accounts in the Administrators group.
    p. Require administrators to log on locally or secure the remote administration solution.

3. **Files and Directories**
    a. Use multiple disks or partition volumes and do not install the Web server home directory on the same volume as the operating system folders.
    b. Contain files and directories on NTFS volumes.
    c. Put Web site content on a non-system NTFS volume.
    d. Create a new site and disable the default site.
    e. Put log files on a non-system NTFS volume but not on the same volume where the Web site content resides.
    f. Restrict the Everyone group (no access to \WINNT\system32 or Web directories).
    g. Ensure Web site root directory has deny write ACE for anonymous Internet accounts.
    h. Ensure content directories have deny write ACE for anonymous Internet accounts.
    i. Remove remote IIS administration application (\WINNT\System32\Inetsrv\IISAdmin).
    j. Remove resource kit tools, utilities and SDKs.
    k. Remove sample applications (\WINNT\Help\IISHelp, \Inetpub\IISSamples).
    l. Remove IP address in header for Content-Location.

4. **Shares**
    a. Remove all unnecessary shares (including default administration shares).
    b. Restrict access to required shares (the Everyone group does not have access).
    c. Remove Administrative shares (C$ and Admin$) if they are not required (Microsoft Management Server (SMS) and Microsoft Operations Manager (MOM) require these shares).
    d. Ports
        i. Restrict Internet-facing interfaces to port 80 (and 443 if SSL is used).
        ii. Encrypt Intranet traffic (for example, with SSL), or restrict Internet traffic
        iii. if you do not have a secure data center infrastructure.

5. **Registry**
    a. Restrict remote registry access.
    b. Secure SAM (HKLM\System\CurrentControlSet\Control\LSA\NoLMHash). This applies only to standalone servers.
    c. Auditing and Logging
        i. Audit failed logon attempts.
        ii. Relocate and secure IIS log files.
        iii. Configure log files with an appropriate file size depending on the application security requirement.
        iv. Regularly archive and analyze log files.
        v. Audit access to the Metabase.bin file.
        vi. Configure IIS for W3C Extended log file format auditing.
        vii. Read How to use SQL Server to analyze Web logs at support.microsoft.com

6. **Sites and Virtual Directories**
    a. Put Web sites on a non-system partition.
    b. Disable "Parent paths" setting.
    c. Remove potentially dangerous virtual directories including IISSamples, IISAdmin, IISHelp and Scripts.
    d. Remove or secure MSADC virtual directory (RDS).
    e. Do not grant included directories Read Web permission.
    f. Restrict Write and Execute Web permissions for anonymous accounts in virtual directories.
    g. Ensure there is script source access only on folders that support content authoring.
    h. Ensure there is write access only on folders that support content authoring and these folders are configured for authentication (and SSL encryption, if required).
    i. Remove FrontPage Server Extensions (FPSE) if not used. If FPSE are used, update and restrict access to them.
    j. Remove the IIS Internet Printing virtual directory.

7. **Script Mappings**
    a. Map extensions not used by the application to 404.dll (.idq, .htw, .ida, .shtml, .shtm, .stm, idc, .htr, .printer).
    b. Map unnecessary ASP.NET file type extensions to “HttpForbiddenHandler” in Machine.config.

8. **ISAPI Filters**
   Remove from the server unnecessary or unused ISAPI filters.

9. **IIS Metabase**
    a. Restrict access to the metabase by using NTFS permissions (%systemroot%\system32\inetsrv\metabase.bin).
    b. Restrict IIS banner information (Disable IP address in content location).

10. **Server Certificates**
    a. Ensure certificate date ranges are valid.
    b. Only use certificates for their intended purpose (For example, the server certificate is not used for e-mail).
    c. Ensure the certificate’s public key is valid, all the way to a trusted root authority.
    d. Confirm that the certificate has not been revoked.

11. **Machine.config**
    a. Map protected resources to HttpForbiddenHandler.
    b. Remove unused HttpModules.
       Disable tracing. <trace enable=”false”/>
    c. Turn off debug compiles.
       <compilation debug=”false” explicit=”true” defaultLanguage=”vb”>

Linux Server Hardening

http://www.cyberciti.biz/tips/linux-security.html

Windows 2003 Server Hardening

http://security.utexas.edu/admin/win2003.html

Windows 2008 Server Hardening

https://wikis.utexas.edu/display/ISO/Windows+2008R2+Server+Hardening+Checklist