Overview

- Secure base
  - Secure the OS
  - Secure the network
  - Minimize other services (access points)
  - Remove defaults
- Secure the network
  - Minimize the web server functionality
- Configuration
  - Global Parameters
  - Minimize web functionality
  - Remove defaults
- Remove defaults
- Add authorization and authentication
- Isolate the parts
- Audit, audit audit

References

- For IIS
  - [http://www.windowsecurity.com/articles/installing_s
  ecurin_iis_servers_part1.html](http://www.windowsecurity.com/articles/installing_s
  ecurin_iis_servers_part1.html)
  - [http://www.serverwatch.com/tutorials/article.php/36
  87211/Securing-the-Ramparts-Within-IIS.htm](http://www.serverwatch.com/tutorials/article.php/36
  87211/Securing-the-Ramparts-Within-IIS.htm)
  - [http://www.serverwatch.com/tutorials/article.php/36
  89626/Securing-IIS-Beyond-the-Web-Server.htm](http://www.serverwatch.com/tutorials/article.php/36
  89626/Securing-IIS-Beyond-the-Web-Server.htm)
- For Apache
  - [http://www.petefreitag.com/item/505.cfm](http://www.petefreitag.com/item/505.cfm)
Secure the OS

- **IIS**
  - Secure the underlying OS
    - Upgrade all patches
    - Turn on updates
    - Subscribe to security bulletins
  - Insure minimal remote access (see services as well)
    - Remove remote desktop connection service
    - Disable remote registry access service. In general, disable any remote Microsoft control services
    - Make sure all system administrators are local administrators (no domain users as admin)
  - Apache
    - Secure the underlying OS
      - Nowhere near as automatic and simple as Microsoft (yum or apt might help)
      - Subscribe to security bulletins
    - Insure minimal remote access (see services as well)
      - At very least disable telnet in favor of ssh
        - Disable SSH Login for root

File System

- **IIS**
  - Remove NTFS write perms everywhere possible
  - Make needed permissions as minimal and explicit as possible
    - E.g. a script does not need read, only access, a text file does not need execute, only read
  - Don’t use virtual directories
- **Apache/Unix**
  - NFS concerns
    - Protections
    - Named script directories
    - Overrides that are allowed
  - Make needed permissions as minimal and explicit as possible

Secure the Network

- **IIS**
  - Establish a firewall that:
    - Limits incoming to DMZ to 80 and 443
    - Limits outgoing to known named secure services fully behind the firewall
  - Run and monitor Intrusion Detection Services
  - Monitor security event files
- **Apache**
  - Establish a firewall that:
    - Limits incoming to DMZ to 80 and 443
    - Limits outgoing to known named secure services fully behind the firewall
  - Run and monitor Intrusion Detection Services
  - Monitor login attempt files
Minimize “Other” Services

- **IIS**
  - Remove ftp, smtp, nntp,
  - Remove remote administration, and remote registry management services etc.
  - The IIS server should never be on a Domain Controller for Active Directory

- **Apache/Linux**
  - Remove telnet, ftp, smtp, nntp, DNS, etc.
  - If possible, remove any shared or network files services

Set Global Configuration Parameters

- **IIS**
  - IIS does not allow as many global modifications as Apache on Unix. Is there a set of registry settings?

- **Apache**
  - Lower the Timeout value
  - Limiting large requests
  - Limiting the size of an XML Body
  - Limiting Concurrency
  - Adjusting KeepAlive settings
  - Limiting the number of request handled per process

Minimize Web Services

- **IIS**
  - Hide IIS information check all server related info. See products such as servermask
  - Relegate scripts to known places
    - Limit scripts and executables to specific directories – don’t use obvious names for these directories
    - Use a non standard names for the script ext
    - Compile scripts to DLLs
    - Minimize permissions on scripts and dlls

- **Apache**
  - Hide Apache information check all server related info, such as
    - ServerSignature Off
    - ServerTokens Prod
    - Server Apache
  - Relegate scripts to known places
  - Protect local changes to files
    - <Directory>
      - Order
      - Deny,Allow
      - Deny from all
      - Options None
      - AllowOverride None
    - <Directory>
      - Order
      - Deny,Allow
      - Deny from all
      - <Directory>
Minimize Web Server Functionality

- **IIS**
  - Turn off directory browsing
  - Turn off server side includes
  - Disable execution of untrusted scripts
  - Disable virtual directories
  - What does it mean and how implemented

- **Apache**
  - Turn off directory browsing
  - Turn off server side includes
  - Turn off CGI execution
  - Turn off support for .htaccess files
  - Disable any unnecessary modules

Reduce Internal Services

- **IIS**
  - Disable:
    - FrontPage 2000 Server Extensions
    - Internet Service Manager (HTML)
    - Visual InterDev RAD Remote Deployment Support
  - Disable unless absolutely needed
    - File Transfer Protocol (FTP) Server
    - NNTP Service - to host newsgroups.
    - SMTP Service - the email server.

- **Apache**
  - Disable:
    - --disable-userdir
    - --disable-autoindex
    - --disable-status
    - --disable-env
    - --disable-cgi
    - --disable-actions
    - --disable-negotiation
    - --disable-alias
    - --disable-includes
    - --disable-filter
    - --disable-version
    - --disable-asis

Remove Default Modules

- **IIS**
  - Obtain and unpack the HiSecWeb.exe file from the Microsoft Web site and harden the site
  - Delete iisadmin, iissamples, inetadmin, scripts, printers
  - Delete ALL default content
  - Delete Temp\* files
  - Delete all .htaccess files
  - Delete \
temp\* files and directories
  - Delete temp\* files and directories

- **Apache**
  - Add more modules that parallel these
Adjust default Account

- **IIS**
  - Delete any unused accounts (Guest and Administrator can’t be deleted)
  - Disable the guest account
  - Rename the Administrator account and assign a strong password
  - Disable the default User account – IUSR_MACHINE
  - Create one or more Custom Anonymous Web accounts – consider multiple accounts for multiple applications

- **Apache**
  - Make sure apache is running under its own user account and group
  - User apache
  - Group apache

Allow for Secure Communication

- **IIS**
  - Make sure SSL is available and used as needed or used all the time
  - Enable authentication to files not to be accessed anonymously

- **Apache**
  - Make sure SSL is available and used as needed or used all the time
  - Establish, via http.conf, htaccess controls with appropriate level of authentication via modules

Isolate the Parts

- **IIS**
  - Put the wwwroot on a separate non-system disk
  - Put the logs on a separate non-system disk – make sure to maximize logging information

- **Apache**
  - Move wwwroot to a separate directory/partition
  - Put the logs on a separate directory/partition – make sure to maximize logging information
Automating Some of the Processes

- **IIS**
  - Run IISLockdown to reduce services (IIS6.0 is installed "locked-down"). It will:
    - Disable ftp, smtp, and nntp
    - Disable script mappings for Index Server, Web Interface, Server side includes, internet data connector, HTML editing and internet printing
    - Remove temporarily IIS Help, Samples, and IIS demo
    - Replaces anonymous access to system utilities
    - Disables WEBDAV
    - Installs the URL Filter ISAPI filter and the 404.dll

- **Apache**
  - Run mod_security
    - Simple filtering
    - Regular Expression based filtering
    - URL Encoding Validation
    - Unicode Encoding Validation
    - Auditing
    - Null byte attack prevention
    - Upload memory limits
    - Server identity masking
    - Built in Chroot support
    - And more

Protect and Audit the Logs

- Set permission to IIS logs to system and local administrators only
- Enable IIS auditing, change to W3 extended logging, and check that the info that is being logged is appropriate
- Make sure only root has read access to apache's config and binaries

Monitor for Patches and Updates

- **IIS**
  - Apply Service Packs and hotfixes.
  - Install high encryption pack.

- **Apache**
  - Apply fixes and upgrades