IIS HARDENING 2

1. Basic Configurations

1.1. Ensure web content is on non-system partition

- Execute the following command to ensure no virtual directories are mapped to the system drive:
    - ***%systemroot%\system32\inetsrv\appcmd list vdir***

1.2. Ensure 'host headers' are on all sites

- IIS Manager > Connections > Sites > Actions > Bindings > Site Bindings > Edit/Add > in host box type a header like malware.org > OK

1.3. Ensure 'directory browsing' is set to disabled

- Click on directory browsing and makes sure that it is disabled
    - OR
- ***%systemroot%\system32\inetsrv\appcmd set config /section:directoryBrowse***
- ***/enabled:false***

1.4. Ensure 'Application pool identity' is configured for all application pools

- ***%systemroot%\system32\inetsrv\appcmd set config /section:applicationPools***
- ***/[name='<your apppool>'].processModel.identityType:ApplicationPoolIdentity***

1.5. Ensure 'unique application pools' is set for sites

- Open IIS Manager >Open the Sites >Select the Site to be changed>In the Actions pane, select Basic Settings > Click the Select… box next to the Application Pool text box > Select the desired Application Pool > OK

1.6. Ensure 'application pool identity' is configured for anonymous user identity

- Open CMD
    - ***%windir%\system32\inetsrv\appcmd set config -section:anonymousAuthentication /username:"" --password***

1.7. Ensure WebDav feature is disabled

- Remove Roles and Features > IIS > Web Server > Common HTTP Features > WebDAV Publishing

2. Configure Authentication and Authorization

2.1. Ensure 'global authorization rule' is set to restrict access

- Select the server > Select Authorization Rules > Remove the "Allow All Users" rule > Click Add Allow Rule > Allow access to the user(s), user groups, or roles that are authorized across all of the web sites

2.2. Ensure access to sensitive site features is restricted to authenticated principals only

- Open IIS Manager and navigate to level with sensitive content > In Features View, double-click Authentication > On the Authentication page, make sure an authentication module is enabled, while anonymous authentication is enabled (Forms Authentication can have anonymous as well) > If necessary, select the desired authentication module, then in the Actions pane,click Enable

2.3. Ensure 'forms authentication' requires SSL

- Open IIS Manager and navigate to the appropriate tier > In Features View, double-click Authentication > On the Authentication page, select Forms Authentication > In the Actions pane, click Edit > Check the Requires SSL checkbox in the cookie settings section, click OK
    - OR
- Config
    - ***<system.web>***
    - ***<authentication>***
    - ***<forms requireSSL="true" />***
    - ***</authentication>***
    - ***</system.web>***

2.4. Ensure 'forms authentication' is set to use cookies

- Open IIS Manager > where Forms Authentication is enabled > In Features View, double-click Authentication > On the Authentication page, select Forms Authentication > In the Actions pane, click Edit > In the Cookie settings section, select Use cookies from the Mode dropdown
- OR
- Config
- ***<system.web>***
- ***<authentication>***
- ***<forms cookieless="UseCookies" requireSSL="true" timeout="30" />***
- ***</authentication>***
- ***</system.web>***

2.5. Ensure 'cookie protection mode' is configured for forms authentication

- ~~***appcmd set config /commit:WEBROOT /section:system.web/authentication /forms.cookieless: UseUri | UseCookies | AutoDetect | UseDeviceProfile***~~
- ~~If that doesn't work~~
- ~~***appcmd set config /commit:WEBROOT /section:system.web/authentication /forms.cookieless:UseDeviceProfile***~~
- If that doesn't work
- Open IIS Manager and navigate to the level where Forms Authentication is enabled > In Features View, double-click Authentication > On the Authentication page, select Forms Authentication > In the Actions pane, click Edit > In the Cookie settings section, verify the drop-down for Protection mode is set for Encryption and validation

2.6. Ensure transport layer security for 'basic authentication' is configured

- Open IIS Manager
  - In the Connections pane on the left, select the server to be configured
  - In the Connections pane, expand the server, then expand Sites and select the site to be configured
  - In the Actions pane, click Bindings; the Site Bindings dialog appears
  - If an HTTPS binding is available, click Close and see below "To require SSL"
    If no HTTPS binding is visible, perform the following steps
- To add an HTTPS binding:
  - In the Site Bindings dialog, click Add; the Add Site Binding dialog appears
  - Under Type, select https
  - Under SSL certificate, select an X.509 certificate
  - Click OK, then close
- To require SSL:
  - In Features View, double-click SSL Settings
  - On the SSL Settings page, select Require SSL.
  - On Windows 2008, also check Require 128-bit SSL.
  - In the Actions pane, click Apply

2.7. Ensure 'passwordFormat' is not set to clear

- In config

- Locate and open the configuration file where the credentials are stored > Find the <credentials> element > If present, ensure passwordFormat is not set to Clear > Change passwordFormat to SHA1

2.8. Ensure 'credentials' are not stored in configuration files
- Locate and open the configuration file where the credentials are stored
- Find the <credentials> element > If present, remove the section

3. ASP.NET Configuration Recommendations

3.1. Ensure 'deployment method retail' is set
- Open the machine.config file located > in:%systemroot%\Microsoft.NET\Framework<bitness (if not the 32bit)>\<framework version>\CONFIG
- > Add the line <deployment retail="true" /> within the <system.web> section
- > If systems are 64-bit, do the same for the machine.config located in: %systemroot%\Microsoft.NET\Framework<bitness (if not the 32 bit)>\<framework version>\CONFIG
-

3.2. Ensure 'debug' is turned off
- Open IIS Manager > Site > In Features View, double-click .NET Compilation
- > On the .NET Compilation page, in the Behavior section, ensure the Debug field is set to False > When finished, click Apply in the Actions pane
-

3.3. Ensure custom error messages are not off
- Open the IIS Manager GUI and navigate to the site to be configured
- 2. In Features View, find and double-click .NET Error Pages icon
- 3. In the Actions Pane, click Edit Feature Settings
- 4. In modal dialog, choose On or Remote Only for Mode settings
- 5. Click OK
-

3.4. Ensure IIS HTTP detailed errors are hidden from displaying remotely
- Open IIS Manager with Administrative privileges
- In the Connections pane on the left, expand the server, then expand the Sites folder
- Select the Web site or application to be configured
- In Features View, select Error Pages, in the Actions pane, select Open Feature
- In the Actions pane, select Edit Feature Settings

- In the Edit Error Pages Settings dialog, under Error Responses, select either Custom error pages or Detailed errors for local requests and custom error pages for remote requests
- Click OK and exit the Edit Error Pages Settings dialog

3.5. Ensure ASP.NET stack tracing is not enabled
- Ensure <deployment retail="true" /> is enabled in the machine.config.
- Remove all attribute references to ASP.NET tracing by deleting the trace and trace enable attributes.

3.6. Ensure 'httpcookie' mode is configured for session state
- Open the IIS Manager GUI and navigate desired server, site, or application 2. In Features View, find and double-click the Session State icon 3. In the Cookie Settings section, choose Use Cookies from the Mode dropdown 4. In the Actions Pane, click Apply
- OR
- %systemroot%\system32\inetsrv\appcmd set config /commit:WEBROOT /section:sessionState /cookieless:UseCookies /cookieName:ASP.NET_SessionID /timeout:20

3.7. Ensure 'cookies' are set with HttpOnly attribute
- In web.config
- ***<configuration>***
- ***<system.web>***
- ***<httpCookies httpOnlyCookies="true" />***
- ***</system.web>***
- ***</configuration>***

3.8. Ensure 'MachineKey validation method - .Net 3.5' is configured
- ***%systemroot%\system32\inetsrv\appcmd set config /commit:WEBROOT /section:machineKey /validation:SHA1***

3.9. Ensure 'MachineKey validation method - .Net 4.5' is configured
- ***%systemroot%\system32\inetsrv\appcmd set config /commit:WEBROOT /section:machineKey /validation:HMACSHA256***

3.10. Ensure global .NET trust level is configured
- ***%systemroot%\system32\inetsrv\appcmd set config /commit:WEBROOT /section:trust /level:Medium***

3.11. Ensure X-Powered-By Header is removed
- In web.config
- ***<security>***

- ***<requestFiltering removeServerHeader ="true"></requestFiltering>***
- ***</security>***
- ***<httpProtocol>***
- ***<customHeaders>***
- ***<remove name="X-Powered-By"/>***
- ***</customHeaders>***
- ***</httpProtocol>***

3.12. Ensure Server Header is removed
- IIS Manager > Connections > HTTP Response Headers > select the X-Powered-By HTTP header
- OR
- Open the Windows Registry Editor.
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HTTP\Parameters.
- Change the DisableServerHeader (REG_DWORD type) registry key from 0 to 1.

4. Request Filtering and other Restriction Modules

4.1. Ensure 'maxAllowedContentLength' is configured
- Request Filtering > Rules > Edit Features Settings > Adjust Maximum allowed length to be 200 (no logic behind this number but if it doesn't work then go up a couple)

4.2. Ensure 'maxURL request filter' is configured
- Request Filtering > Rules > Edit Features Settings > Adjust Maximum allowed length to be 200

4.3. Ensure 'MaxQueryString request filter' is configured
- Request Filtering > Rules > Edit Features Settings > Adjust Maximum allowed length to be 200

4.4. Ensure non-ASCII characters in URLs are not allowed
- Request Filtering > Edit Feature Settings > Make sure high-bit characters is unchecked

4.5. Ensure Double-Encoded requests will be rejected
- In the web config
- ***<configuration>***
- ***<system.webServer>***
- ***<security>***

- ***<requestFiltering***
- ***allowDoubleEscaping="false">***
- ***</requestFiltering>***
- ***</security>***
- ***</system.webServer>***
- ***</configuration>***

4.6. Ensure 'HTTP Trace Method' is disabled
- Request Filtering > Deny Verb > TRACE

4.7. Ensure Unlisted File Extensions are not allowed
- Request Filtering > File Name Extensions > Type extensions you want to allow or deny

4.8. Ensure Handler is not granted Write and Script/Execute
- Command Prompt (AS ADMIN) > cd %systemdrive%\inetpub\wwwroot (or wherever your root config is)
  - OR cd %Windir%\system32\inetsrv\config
- Edit the config file in notepad then find ***handlers accessPolicy***
- Type ***<handlers accessPolicy="Read, Script">***

4.9. Ensure ‘notListedIsapisAllowed’ is set to false
- Select Host Machine in IIS Manager under Connections Pane > Features > ISAPI and CGI Restrictions > Actions > Edit Feature Settings > Edit ISAPI and CGI Restrictions Settings
- OR
- Add these lines to the main config
  - ***<system.webserver>***
  - ***<handlers accessPolicy="Read, Script">***
  - ***</handlers>***
  - ***</system.webserver>***
-

4.10. Ensure ‘notListedCgisAllowed’ is set to false
- ***%systemroot%\system32\inetsrv\appcmd.exe set config -section:system.webServer/security/isapiCgiRestriction /notListedCgisAllowed:false***

4.11. Ensure ‘Dynamic IP Address Restrictions’ is enabled
- Install IP & Domain Restrictions > IP Address and Domain Restrictions > Edit in Actions Pane > 5 concurrent requests > 20 max number > timeperiod 200

7. Transport Encryption

7.1. Ensure HSTS Header is set

- Run the IIS manager.
- Select your site
- Select HTTP REsponse Headers.
- Click on Add in the Actions section.
- In the Add Custom HTTP Response Header dialog, add the following values:
- For Name: Strict-Transport-Security
- For Value: max-age=15552001; includeSubDomains; preload

NOTE THE BELOW MUST BE EDITED IN THE REGISTRY AND THE HOST MACHINE MUST BE REBOOTED

Also HKEY_LOCAL_MACHINE/System…..
Also you have to change the keys if they are there :)

7.2. Ensure SSLv2 is Disabled

- Set the following key to 0
- HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server\Enabled
-

7.3. Ensure SSLv3 is Disabled

- Set the following key to 0
- HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server\Enabled

7.4. Ensure TLS 1.0 is Disabled

- Set the following key to 0
- HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server\Enabled
- Set the following key to 1
- HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server\DisabledByDefault
-

7.5. Ensure TLS 1.1 is Disabled

- Set the following key to 0
- HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server\Enabled

7.6. Ensure TLS 1.2 is Enabled
- If there is HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
- find TLS then
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client] "DisabledByDefault"=dword:00000000 "Enabled"=dword:00000001
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server] "DisabledByDefault"=dword:00000000 "Enabled"=dword:00000001
-

7.7. Ensure NULL Cipher Suites is Disabled
- Set the following key to 0
- HKLM System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\NULL\Enabled

7.8. Ensure DES Cipher Suites is Disabled
- Set the following key to 0
- HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56\Enabled

7.9. Ensure RC Cipher Suites is Disabled
- Set the following key to 0
- HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 40/128\Enabled
- HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 56/128\Enabled

7.10. Ensure AES 128/128 Cipher Suite is Disabled
- Set the following key to 0xFFFFFFFF
- HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 128/128\Enabled

7.11. Disable RC4
- Keys should be located under HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4
- Set them all to 0

7.13 Ensure AES 256/256 Cipher Suite is Enabled

- Set to 0xFFFFFFFF
- HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 256/256\Enabled
-

7.14 Ensure TLS Cipher Suite Ordering is Configured

- Check the following key
- HKLM\System\CurrentControlSet\Control\Cryptography\Configuration\Local\SSL\00010002\Functions
- Set to
    - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256
    - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
    - TLS_RSA_WITH_AES_256_CBC_SHA
    - TLS_RSA_WITH_AES_128_CBC_SHA
    - TLS_RSA_WITH_3DES_EDE_CBC_SHA

HSTS

- Run the IIS manager.
- Select your site
- Select HTTP REsponse Headers.
- Click on Add in the Actions section.
- In the Add Custom HTTP Response Header dialog, add the following values:
    - For Name: Strict-Transport-Security
    - For Value: max-age=15552001; includeSubDomains; preload