CIS Microsoft IIS 10 Benchmark: Hardening Recommendations

* Ensure Web Content is non-system partition: Isolating web content from system files will reduce the possibility of web sites and application from using all disk space, and file 10 vulnerability in the wen site.
* Ensure host headers are on all sites: This will reduce the probability of DNS rebinding attacks, and IP-based scans.
* Ensure directory browsing is set to disabled: This can help reduce the probability of disclosing sensitive content that is available via IIS,
* Ensure application pool identity is configured for all applications: This reduces the potential harm the identity could cause should the application become compromised.
* Ensure unique application pools is set for sites: This can improve server and application performance and security.
* Ensure application pool identity is configured for anonymous user identity: This will help ensure site isolation.
* Ensure forms authentication require SSL: This will protect the confidentiality of credentials during the login process, helping mitigate the risk of stolen user information.
* Ensure forms authentication is set to use cookies: This will help mitigate the risk of session hi-jacking attempts.
* Ensure cookie protection mode is configured for forms authentication: By encrypting and validating the cookie, the confidentiality and integrity of data is assured.
* Ensure transport layer security for basic authentication is configured: This will help prevent the clear text from being intercepted.
* Ensure passwordFormat is not set to clear: This will protect authentication credentials.
* Ensure credentials are not stored in configuration files: This prevents credentials from being stored in configuration files.
* Ensure deployment method retail is set: This switch eliminates the risk of leakages if tracing or debug were left enabled.
* Ensure debug is turned off: Reduces risk of detailed error info from displaying unintentionally.
* Ensure custom error messages are not off and IIS HTTP detailed errors are hidden from displaying remotely: Configure errors to only display relevant information about the issue experienced. Make sure that errors do not display too much information like usernames, passwords, servers IP address among other information that hackers may use exploit the web server.
* Ensure ASP.NET stack tracing is not enabled: Trace information should not be open to anyone who views the site pages.
* Ensure httpcookie mode is configured for session state: Mitigates risk of session hi-jacking attempts.
* Ensure cookies are set with HttpOnly attribute: Cookies marked with this flag cannot be accessed from the client side.
* Ensure MachineKey validation method - .Net 3.5 and .Net 4.5 is configured: Provides protection to the viewstate, ensure SHA-2 is used for .Net 4.5 for the strongest hashing algorithm.
* Ensure global .NET trust level is configured: Set the minimum level required for compatibility with applications.
* Ensure maxURL and MaxQueryString request filter is configured: Maintains availability of resources while mitigating the risk of buffer overflow attacks.
* Ensure non-ASCII characters in URLs are not allowed: Reduces the potential attack surface.
* Ensure Double-Encoded requests will be rejected: Prevents attacks based on reliance of URLs meant to contain double-encoded requests.
* Ensure HTTP Trace Method is disabled: Often used to gain access to information like cookies and authentication data.
* Ensure Unlisted File Extensions are not allowed: Allowing only authorized file extensions reduces the attack surface.
* Ensure Handler is not granted Write and Script/Execute: Reduces risk of the handler running malicious code.
* Ensure notListedIsapisAllowed and notListedCgisAllowed is set to false: Prevents malicious ISAPI extensions and CGI scripts from running.
* Ensure Default IIS web log location is moved: Reduces risk of malicious altering or loss of logs.
* Ensure Advanced IIS logging is enabled: Use logging to see visitors who have been accessing the web server and help track whenever you suspect someone has been using your server without authorization.
* Ensure FTP requests are encrypted: Using SSL encrypts the transmission from point to point.
* Ensure SSLv2 and SSLv3 is disabled: Disable weak protocols to ensure security and integrity of data.
* Ensure TLS 1.2 is enabled: Ensures proper confidentiality and integrity of data in transit.
* Ensure NULL Cipher Suites, DES Cipher Suites, RC4 Cipher Suites, and Triple DES Cipher Suite is disabled: Increases ability to maintain data confidentiality and integrity.
* Ensure AES 256/256 Cipher Suite is enabled: Aids in ensuring the confidentiality and integrity of data in transit.
* Ensure TLS Cipher Suite ordering is configured: Order suites from strongest to weakest to ensure the most secure configuration is used between server and client.

**References**

CIS Microsoft IIS 10 Benchmark. (2017, March 31).

https://hostadvice.com/how-to/how-to-harden-windows-iis/