**Virtual Directory**

|  |  |
| --- | --- |
| **Security Specifications** | **Status** |
| Ensure restriction is enabled to those directories that allows anonymous access |   |
| Ensure IISAdmin, IISHelp, IISamples directory are removed |   |
| Confirm PARENT PATH configuration is disabled |   |
| Ensure unused Front pages extension is removed |   |
| Ensure website directories are dislocated from the system partition drive |   |
| Ensure directory traversing is disabled (uncheck write permission) |   |
| Ensure other unused utilities such resource kit, SDK are detached |   |

**Machine Configuration File**

|  |  |
| --- | --- |
| **Security Specifications** | **Status** |
| Ensure DEBUG is turned-off in WEB.CONFIG file |   |
| Ensure TRACE is set to false or disabled |   |
| Ensure unnecessary HTTP Modules are removed |   |

**Secure Communication**

|  |  |
| --- | --- |
| **Security Specifications** | **Status** |
| Ensure HTTP requests are filtered or categorized |   |
| Ensure HTTPs is enable, in case if your website deals with sensitive data |   |
| Ensure Server Certificates is updated and issued by trusted organization |   |
| Ensure Certificates has not withdrawn |   |
| In case of Remote administration, ensure proper time-outs and encryption is configured |   |
| Ensure communication is happens using only port 80 or 443 |   |
| Ensure that IPSec is formed in the network for secure communication |   |

**Logging and Audit**

|  |  |
| --- | --- |
| **Security Specifications** | **Status** |
| Ensure Failed Logon Attempts are regularly inspected |   |
| Ensure Log files are properly maintained and audited |   |
| Confirm W3C extended format is enabled for auditing |   |

**IIS Metabase and Filters**

|  |  |
| --- | --- |
| **Security Specifications** | **Status** |
| Ensure Banner grabbing is disabled |   |
| Ensure File (%systemroot%\system32\inetsrv\metabase.bin) access is restricted |   |
| Ensure unused extensions (.shtml, .hta, .htw, .stm,,) are removed |   |
| Ensure unemployed ISAPI filters are disabled or removed. |   |
| Ensure "Forbidden Handler" is mapped to unemployed ASP.NET files extension |   |

**Server Accounts**

|  |  |
| --- | --- |
| **Security Specifications** | **Status** |
| Ensure anonymous logon is disabled |   |
| Ensure unused IUSR\_MACHINE account is disabled |   |
| Ensure a solitary administrator account only |   |
| Ensure administrator account is properly hardened by strong password scheme |   |
| Ensure GUEST account is disabled |   |
| Ensure remote logon is disabled |   |
| Ensure ASP.NET process account is configured to least access |   |
| Ensure anyone couldn't login locally except administrator |   |

**Code Access Security**

|  |  |
| --- | --- |
| **Security Specifications** | **Status** |
| Confirm CAS is enabled |   |
| Confirm source code is obfuscated |   |
| Confirm custom error page is installed on server |   |
| Confirm permissions removed from Internet and Intranet zone |   |

**System Configuration**

|  |  |
| --- | --- |
| **Security Specifications** | **Status** |
| Confirm ASP.NET state service is disabled |   |
| Confirm Remote Registry Administration is disabled |   |
| Confirm WebDAW service is disabled |   |
| Confirm FTP and SMTP services are disabled |   |
| Confirm SMB service is disabled |   |
| Confirm All Redundant share's (C$, D$,..) is removed |   |
| Confirm Remote Administration by TELNET is disabled |   |
| Confirm only essential System Services given least privilege |   |
| Confirm redundant system services are stop |   |
| Ensure IIS is not installed on domain controller |   |
| Ensure IDS is installed in the network perimeter |   |
| Ensure that IIS server is configured inside DMZ |   |

**Server Updates**

|  |  |
| --- | --- |
| **Security Specifications** | **Status** |
| Ensure Windows Operating System is updated |   |
| Ensure .NET Framework is Updated |   |
| Ensure IIS web server is duly patched |   |
| Ensure MBSA is configured and running regularly |   |
| Ensure EMET is installed on server and enabled |   |
| Ensure Microsoft Notification Service is Enabled |   |
| Ensure effective Anti-virus is installed and running |  |