Center for
Internet Security

CIS Microsoft SharePoint 2016 Benchmark

v1.0.0 - 08-17-2017

Table of Contents

Overview

This document, Security Configuration Benchmark for Microsoft Office SharePoint Server 2016, provides prescriptive guidance for establishing a secure configuration posture for Microsoft Office SharePoint Server 2016.

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Microsoft Office SharePoint Server 2016 and Windows SharePoint Services 3.0 (WSS) running on Microsoft Windows Server 2016.

Consensus Guidance

This benchmark was created using a consensus review process comprised of subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus process, please visit https://community.cisecurity.org.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
Monospace font	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Scoring Information

A scoring status indicates whether compliance with the given recommendation impacts the assessed target's benchmark score. The following scoring statuses are used in this benchmark:

Scored

Failure to comply with "Scored" recommendations will decrease the final benchmark score. Compliance with "Scored" recommendations will increase the final benchmark score.

Not Scored

Failure to comply with "Not Scored" recommendations will not decrease the final benchmark score. Compliance with "Not Scored" recommendations will not increase the final benchmark score.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile apply to Microsoft SharePoint 2016 running on Microsoft Windows Server 2016 and intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not inhibit the utility of the technology beyond acceptable means.

Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Editor
Eric Ibison
Derek Ho
Hardeep Mehrotara CISSP, CISA, CICP

Recommendations

1 Settings

1.1 Ensure access to SharePointEmailws.asmx is limited to only the server farm account (Not Scored)

Profile Applicability:

- Level 1

Description:

Restrict access to the Microsoft SharePoint Directory Management Service by securing the file associated with this service, which is SharePointEmailws.asmx. Only the SharePoint server farm account requires access.

Rationale:

SharePoint 2013 includes an internal service, the Microsoft SharePoint Directory Management Service, for creating e-mail distribution groups. When you configure e-mail integration, you have the option to enable the Directory Management Service feature, which lets users create distribution lists. When users create a SharePoint group and they select the option to create a distribution list, the Microsoft SharePoint Directory Management Service creates the corresponding Active Directory distribution list in the Active Directory environment. Creating distribution lists in Active Directory should be limited to only this account.

Audit:

Navigate to the directory `%COMMONPROGRAMFILES%\Microsoft Shared\web server extensions\12\ISAPI`

1. Find the `SharePointEmailws.asmx` file used by the `Microsoft SharePoint Directory Management Service` in the following
2. Right-click on the `File` and view the `Properties`.
3. On the `Security` tab verify that only the `Microsoft SharePoint Directory Management Service` has access to modify the file.

Remediation:

Navigate to the directory `%COMMONPROGRAMFILES%\Microsoft Shared\web server extensions\12\ISAPI`

1. Find the `SharePointEmailws.asmx` file used by the `Microsoft SharePoint Directory Management Service` in the following
2. Right-click on the `File` and view the `Properties`.
3. On the `Security` tab verify that only the `Microsoft SharePoint Directory Management Service` has access to modify the file.

References:

1. https://technet.microsoft.com/es-es/library/cc262849(v=office.16).aspx

CIS Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

1.2 Ensure that the SharePoint Central Administration Site is TLS-enabled (Not Scored)

Profile Applicability:

- Level 1

Description:

Transport Layer Security (TLS) provides protection when communicating over the internet. Traffic is encrypted for portions of information transportation. Ensure that the Central Administration site is configured to be used with TLS.

Rationale:

The SharePoint Central Administration site allows an administrator to manage settings for the Web server and virtual servers. TLS protects this critical data by encrypting the traffic that is transmitted over the network.

Audit:

Navigate to Internet Information Services (IIS) Manager.

1. Locate the `SharePoint Central Administration v4` from the `Sites` category and verify that it is configured with an `HTTPS binding`.
2. Locate the `SharePoint Central Administration v4` from the `Sites` category
3. Double click on the `Actions` pane, in the `Edit Site` section.
4. Click the `Bindings` link.
5. In the `Site Bindings` dialog, select the `HTTPS binding` and click `Edit`
6. In the `Edit Site Binding` dialog, ensure that the `Port, Hostname and SSL Certificate` settings field have entries.

Remediation:

An SSL certificate must be acquired before enabling TLS. For more information about SSL certificates, see related topics in IIS 8.0 Help.
The Central Administration site must also be first configured to use port 443 and HTTPS. To configure this, execute the following Windows PowerShell command:

```
Set-SPCentralAdministration -Port 443
```

Navigate to Internet Information Services (IIS) Manager.

1. Locate the `SharePoint Central Administration v4` from the `Sites` category and verify that it is configured with an `HTTPS binding`.
2. Locate the `SharePoint Central Administration v4` from the `Sites` category.
3. Double click on the `Actions` pane, in the `Edit Site` section.
4. Click the `Bindings` link.
5. In the `Site Bindings` dialog, select the `HTTPS binding` and click `Edit`.
6. In the `Edit Site Binding` dialog, ensure that the `Port, Hostname and SSL Certificate` settings fields accordingly.

References:

1. https://technet.microsoft.com/en-us/library/cc262849.aspx

CIS Controls:

14.2 Encrypt All Sensitive Information Over Less-trusted Networks
All communication of sensitive information over less-trusted networks should be encrypted. Whenever information flows over a network with a lower trust level, the information should be encrypted.

1.3 Ensure specific whitelisted IP addresses, IP address ranges, and/or domains are set (Not Scored)

Profile Applicability:

- Level 1

Description:

Access to the SharePoint web application should be restricted to a certain group of users. Typically, this is done through restricting IP addresses to selectively allow known and approved user populations.

Rationale:

Restricting access to the SharePoint site minimizes the risks due to exposure of the application to unknown user populations. Risks including loss of confidentiality and integrity of stored data could be drastically reduced.

Audit:

Navigate to Internet Information Services (IIS) Manager.

1. Locate the `SharePoint Central Administration v4` from the Sites category.
2. Right-click the `Web site` or `Folder`, and then click `Properties`.
3. Click the `Directory Security panel`.
4. Click `Denied Access`.
5. Ensure that the lists of specific whitelisted IP addresses, IP address ranges, and/or domains are adequate.

Remediation:

Start Internet Information Services (IIS) Manager.

1. Locate the `SharePoint Central Administration v4` from the `Sites` category.
2. Right-click the `Web site` or `Folder`, and then click `Properties`.
3. Click the `Directory Security panel`.
4. Click `Denied Access`.
5. To add single IP addresses for whitelisting, click `Single computer` and enter the `whitelisted IP address`.
6. To add a range of IP addresses for whitelisting, click `Group of computers` and enter the `whitelisted IP address range`.
7. To add a specific domain for whitelisting, click `Domains` and enter the `whitelisted domain`.

References:

1. https://support.microsoft.com/en-us/help/324066/how-to-restrict-site-access-by-ip-address-or-domain-name
2. https://technet.microsoft.com/en-us/library/cc262849.aspx

CIS Controls:

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

1.4 Ensure that the underlying Internet Information Services (IIS) Authentication module is set to use Kerberos as its Authentication Provider (Not Scored)

Profile Applicability:

- Level 1

Description:

The Kerberos protocol is a more secure protocol than NTLM and is based on ticketing. In this scheme, a user provides a valid user name and password to an authentication server. Then, the authentication server grants the user a ticket. The ticket can be used on the network to request network resources.

Rationale:

The NTLM protocol has a number of vulnerabilities where a malicious attacker can use a pass the hash attack to gain access to user credentials. The Kerberos protocol is a more secure protocol based on a ticketing system and is recommended.

Audit:

Navigate to the `Inetpub\Adminscripts` folder using a `Command Prompt` window on the server that is running `IIS`

1. Enter the command `cd Drive:\inetpub\adminscripts` in the command prompt window.
   Note In this command, Drive is the drive where Microsoft Windows is installed.
2. Enter the command `cscript adsutil.vbs get w3svc/##/root/NTAuthenticationProviders` in the command prompt window.
   Note In this command, ## is the virtual server ID number. The virtual server ID number of the Default Web site in IIS is 1.
3. Enter the command `cscript adsutil.vbs get w3svc/##/root/NTAuthenticationProviders`
   Note In this command, ## is the virtual server ID number.
4. Verify `Negotiate,NTLM` is set as the `Authentication Provider`

Remediation:

Navigate to the `Inetpub\Adminscripts` folder using a `Command Prompt` window on the server that is running `IIS`

1. Enter the command `cd Drive:\inetpub\adminscripts` in the command prompt window.
   Note In this command, Drive is the drive where Microsoft Windows is installed.
2. Enter the command `cscript adsutil.vbs get w3svc/##/root/NTAuthenticationProviders` in the command prompt window.
   Note In this command, ## is the virtual server ID number. The virtual server ID number of the Default Web site in IIS is 1.
3. Enter the command `cscript adsutil.vbs set w3svc/##/root/NTAuthenticationProviders Negotiate,NTLM`
   Note In this command, ## is the virtual server ID number.
4. Enter the following command in the command prompt window `iisreset` to reset IIS.

Impact:

A malicious attacker could exploit vulnerabilities in old NTLM protocols and gain access to user and administrative credentials.

Default Value:

NTLM

References:

1. https://msdn.microsoft.com/en-us/library/cc339532(v=vs.90).aspx

CIS Controls:

16.9 Configure Account Access Centrally
Configure access for all accounts through a centralized point of authentication, for example Active Directory or LDAP. Configure network and security devices for centralized authentication as well.

2 Access and Permissions

2.1 Ensure 'Block File Types' is configured to match the enterprise blacklist (Scored)

Profile Applicability:

- Level 1

Description:

A common tactic of malware is to identify the type of malicious code protection software running on the system and deactivate it. Malicious code includes viruses, worms, Trojan horses, and Spyware.

Rationale:

Malicious code protection software must be protected to prevent a non-privileged user or malicious piece of software from disabling the protection mechanism.

Audit:

Review the SharePoint server configuration to ensure non-privileged users are prevented from circumventing malicious code protection capabilities.
Confirm that the list of blocked file types configured in Central Administration matches the enterprise "blacklist".
Navigate to `Central Administration`.

1. Click `Security`, and then click `Define blocked file type`.
2. To change the web application, click the link next to `Web Application:` and then click `Change Web Application`.
3. In the Select Web Application dialog, click an app.
4. On the `Blocked File Types` page compare the list of blocked file types to those listed in the enterprise blacklist.
5. Repeat check for each web application.

Remediation:

Navigate to `Central Administration`.

1. Click `Security`, and then click `Define blocked file type`.
2. To change the web application, click the link next to `Web Application:` and then click `Change Web Application`.

3. In the Select Web Application dialog, click an app.
4. On the `Blocked File Types` page to add a file to block, type a file extension (with the period), one per line.
5. Add all file types listed in the enterprise blacklist.
6. Repeat check for each web application.

References:

1. https://support.office.com/en-us/article/Types-of-files-that-cannot-be-added-to-a-list-or-library-30be234d-e551-4c2a-8de8-f8546ffbf5b3?ui=en-US&rs=en-US&ad=US&fromAR=1#ID0EAADAAA=2016

CIS Controls:

8 Malware Defenses
Malware Defenses

2.2 Ensure the SharePoint farm service account (database access account) is configured with the minimum privileges for the local server. (Scored)

Profile Applicability:

- Level 1

Description:

The SharePoint farm service account (database access account) must be configured with the minimum privileges for the local server.

Rationale:

Separation of duties is a prevalent Information Technology control implemented at different layers of the information system including the operating system and in applications. It serves to eliminate or reduce the possibility that a single user may carry out a prohibited action. Separation of duties requires the person accountable for approving an action not be the same person who is tasked with implementing the action.

This requirement is intended to limit exposure due to user accounts being used to operate from within a privileged account or role. Limiting the access and permissions of privileged accounts to the minimum required, reduces exposure if the account is compromised and provides forensic history of activity when operating from these accounts.

This policy limits the Farm Account privileges in AD. However, default permissions for this account are configured by the SharePoint Products Configuration Wizard during product installation. This account is referred to during the installation as the Database Access account. By default, the account is used as the service account for the SharePoint Timer Service and the SharePoint Central Administration Web Site Application Pool. These settings should not be changed. Furthermore, this account should not be used as the service account for non-privileged services, applications, or application pools.

Audit:

Review the SharePoint server configuration to verify the farm service account (database access account) is configured with the minimum privileges for the local server.

1. On the server(s) where the SharePoint software is installed, navigate to `Server Manager > Local Users and Groups`.

2. Select the Member of tab and verify this account is only a member of the `WSS_RESTRICTED_WP`, `WSS_ADMIN_WPG`, and `WSS_WPG` groups.
3. Select the other tabs in this area to verify no other services or permissions are configured for this account.

If the farm service account is a member of any other groups than `WSS_RESTRICTED_WPG`, `WSS_ADMIN_WPG`, or `WSS_WPG` on the local server where SharePoint is installed, this is a finding.

Remediation:

1. On the server(s) where the SharePoint software is installed, navigate to `Server Manager > Local Users and Groups`.
2. Select the Member of tab and ensure this account is only a member of the `WSS_RESTRICTED_WPG`, `WSS_ADMIN_WPG`, and `WSS_WPG` groups.
3. Select the other tabs in this area to ensure there are no other services or permissions are configured for this account.

References:

1. https://technet.microsoft.com/en-us/library/cc678863(v=office.16).aspx

CIS Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

2.3 Ensure the SharePoint setup account is configured with the minimum privileges in Active Directory. (Not Scored)

Profile Applicability:

- Level 1

Description:

The SharePoint setup account must be configured with the minimum privileges in Active Directory.

Rationale:

Separation of duties is a prevalent Information Technology control implemented at different layers of the information system including the operating system and in applications. It serves to eliminate or reduce the possibility that a single user may carry out a prohibited action. Separation of duties requires the person accountable for approving an action not be the same person who is tasked with implementing the action.

This requirement is intended to limit exposure due to user accounts being used to operate from within a privileged account or role. Limiting the access and permissions of privileged accounts to the minimum required, reduces exposure if the account is compromised and provides forensic history of activity when operating from these accounts.

This policy limits the setup account privileges in AD. However, default permissions for this account are configured by the SharePoint Products Configuration Wizard during product installation. This account is referred to during the installation as the "Database Access" account. By default, the account is used as the service account for the SharePoint Timer Service and the SharePoint Central Administration Web Site Application Pool. These settings should not be changed. Furthermore, this account should not be used as the service account for non-privileged services, applications, or application pools.

Audit:

Review the SharePoint server configuration to ensure the setup account is configured with the minimum privileges in Active Directory.
Verify the account has least privilege in Active Directory.

1. Navigate to `Active Directory Users and Computers > Users`.
2. Double click on the setup user account to view the account properties.
3. Select the `Members of` tab and verify this account is a member of the `Domain Users` group only.

4. Select the other tabs in this area to verify no other services or permissions are configured for this account.

Remediation:

1. Navigate to `Active Directory Users and Computers > Users`.
2. Double click on the setup user account to view the account properties.
3. Select the `Members of` tab and remove and group that is not `Domain Users`.
4. Select the other tabs in this area to verify no other services or permissions are configured for this account.

References:

1. https://technet.microsoft.com/en-us/library/cc678863(v=office.16).aspx#Section2

CIS Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

2.4 Ensure SharePoint provides the ability to prohibit the transfer of unsanctioned information in accordance with security policy. (Not Scored)

Profile Applicability:

- Level 1

Description:

SharePoint must provide the ability to prohibit the transfer of unsanctioned information in accordance with security policy.

Rationale:

The application enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information.

Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) employing rule sets or establishing configuration settings restricting information system services, providing a packet-filtering capability based on header information or message-filtering capability based on content (e.g., using key word searches or document characteristics).

Actions to support this requirement include, but are not limited to checking all transferred information for malware, implementing dirty word list searches on transferred information, and applying the same protection measures to metadata (e.g., security attributes) that is applied to the information payload.

Audit:

Review the SharePoint server configuration to ensure the transfer of unsanctioned information in accordance with security policy is prohibited.
An IRM must be enabled in SharePoint. The Windows Rights Management Services (RMS) (or a comparable IRM product) can either be located through Active Directory or specified.
`Central Administration > Security`

On the Security page, in the Information policy list, click `Configure information rights management`.
If "Do not use IRM on this server" is selected or if a configuration error message is displayed (such as "... IRM will not work until the client is configured properly"), this is a finding.

Remediation:

An IRM must be enabled in SharePoint. The Windows Rights Management Services (RMS) (or a comparable IRM product) can either be located through Active Directory or specified.

CIS Controls:

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

2.5 Ensure the SharePoint setup account is configured with the minimum privileges on the SQL server. (Scored)

Profile Applicability:

- Level 1

Description:

The SharePoint setup account must be configured with the minimum privileges on the SQL server.

Rationale:

Having the SharePoint setup account be configured with the minimum necessary privileges on the SQL server would help reduce the risks related to account misuse. When excessive roles are given to any SQL server accounts, the potential impact of actions performed through the account increases. Malicious action performed by compromised accounts in the control of an attacker, or even honest mistakes and gaffes performed by valid users can have vast devastating consequences, depending on the roles and privileges given.

Audit:

The SharePoint setup account must be configured with the minimum privileges on the SQL server.

1. Launch `SQL Server Management Console` and navigate to `Security > Logins`.
2. Select the SharePoint Setup User account.
3. Click on `Server Roles` and verify only `db_owner`, `dbcreator`, and `securityadmin` are checked.

Remediation:

1. Launch `SQL Server Management Console` and navigate to `Security > Logins`.
2. Select the SharePoint Setup User account.
3. Click on `Server Roles` and check only `db_owner`, `dbcreator`, and `securityadmin`.

References:

1. https://technet.microsoft.com/en-us/library/ee662513(v=office.16).aspx

CIS Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

2.6 Ensure the SharePoint farm service account (database access account) is configured with the minimum privileges on the SQL server. (Scored)

Profile Applicability:

- Level 1

Description:

The SharePoint farm service account (database access account) must be configured with the minimum privileges on the SQL server

Rationale:

Separation of duties is a prevalent Information Technology control implemented at different layers of the information system including the operating system and in applications. It serves to eliminate or reduce the possibility that a single user may carry out a prohibited action. Separation of duties requires the person accountable for approving an action not be the same person who is tasked with implementing the action.

This requirement is intended to limit exposure due to user accounts being used to operate from within a privileged account or role. Limiting the access and permissions of privileged accounts to the minimum required, reduces exposure if the account is compromised and provides forensic history of activity when operating from these accounts.

This policy limits the Farm Account privileges in AD. However, default permissions for this account are configured by the SharePoint Products Configuration Wizard during product installation. This account is referred to during the installation as the Database Access account. By default, the account is used as the service account for the SharePoint Timer Service and the SharePoint Central Administration Web Site Application Pool. These settings should not be changed. Furthermore, this account should not be used as the service account for non-privileged services, applications, or application pools.

Audit:

Review the SharePoint server configuration to ensure the farm service account (database access account) is configured with minimum privileges on the SQL server.

1. Launch the `SQL Server Management Console` and navigate to `Security > Logins`.
2. Select the SharePoint farm service account.

3. Click on `Server Roles` and verify that only `db_owner`, `dbcreator`, and `securityadmin` are checked.

Remediation:

1. Launch the `SQL Server Management Console` and navigate to `Security > Logins`.
2. Select the SharePoint farm service account.
3. Click on Server Roles and check ONLY `db_owner`, `dbcreator`, and `securityadmin`.

References:

1. https://technet.microsoft.com/en-us/library/cc678863(v=office.16).aspx

CIS Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

2.7 Ensure only the server farm account has access to SharePointEmailws.asmx (Scored)

Profile Applicability:

- Level 1

Description:

SharePoint 2016 includes an internal service, the Microsoft SharePoint Directory Management Service, for creating e-mail distribution groups. When you configure e-mail integration, you have the option to enable the Directory Management Service feature, which lets users create distribution lists. When users create a SharePoint group and they select the option to create a distribution list, the Microsoft SharePoint Directory Management Service creates the corresponding Active Directory distribution list in the Active Directory environment.

Rationale:

The ability to create distribution lists should be limited to only those accounts that require the ability to create lists. Restricting the accounts that can access SharePointEmailws.asmx accomplishes that.

Audit:

1. Locate the `SharePointEmailws.asmx` file in Windows Explorer
2. Right-click on the file and choose `Properties`
3. Click on the `Security` tab
4. Validate only the server farm account has read permissions to the file.

Remediation:

1. Locate the `SharePointEmailws.asmx` file in Windows Explorer
2. Right-click on the file and choose `Properties`
3. Click on the `Security` tab
4. Set the permissions so that only the server farm account has read permissions to the file.

References:

1. https://technet.microsoft.com/en-us/library/cc262849(v=office.16).aspx

CIS Controls:

5.1 Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

2.8 Ensure a separate organizational unit (OU) in Active Directory exists for SharePoint 2016 objects. (Scored)

Profile Applicability:

- Level 1

Description:

SharePoint 2016 includes an internal service, the Microsoft SharePoint Directory Management Service, for creating e-mail distribution groups. When you configure e-mail integration, you have the option to enable the Directory Management Service feature, which lets users create distribution lists. When users create a SharePoint group and they select the option to create a distribution list, the Microsoft SharePoint Directory Management Service creates the corresponding Active Directory distribution list in the Active Directory environment.

Rationale:

The recommendation is to set up a separate organizational unit (OU) in Active Directory for SharePoint 2016 objects. Only this OU should allow write access to the account that is used by the Microsoft SharePoint Directory Management Service.

Audit:

1. Open `Active Directory Users and Computers` on a domain controller within the Active Directory domain used for SharePoint.
2. Validate there is a separate OU created for use only with SharePoint 2016 objects.
3. Validate that only the account used for the Microsoft SharePoint Directory Management Servers has `write` access to that OU.

Remediation:

1. Open `Active Directory Users and Computers` on a domain controller within the Active Directory domain used for SharePoint.
2. Validate there is a separate OU created for use only with SharePoint 2016 objects, if there is not a separate OU create one.
3. Modify the separate OU so that only the account used for the Microsoft SharePoint Directory Management Servers has `write` access to that OU.

References:

1. https://technet.microsoft.com/en-us/library/cc262849(v=office.16).aspx

CIS Controls:

16 Account Monitoring and Control
Account Monitoring and Control

2.9 Ensure the SharePoint Central Administration site is not accessible from Extranet or Internet connections (Scored)

Profile Applicability:

- Level 1

Description:

The SharePoint central administration site should be configured so that its ports and interfaces are not accessible to untrusted external or internet connections.

Rationale:

The central administration site is a critical component to the management of the SharePoint platform, allowing administrators to perform a variety of administration tasks, including creating and managing SharePoint Web Applications, Site Collections and Service Applications. Minimizing unnecessary exposure to this site would certainly help mitigate risks to the SharePoint platform.

Audit:

- On the drive where SharePoint Products and Technologies is installed, open a command-line window and type the following command:

```
cd %CommonProgramFiles%\Microsoft Shared\Web Server Extensions\12\bin
```

- Determine the current port number for the Central Administration Web site, by typing the following command:

```
stsadm -o getadminport
```

- Verify through your firewall settings that the SharePoint system and the identified port is not exposed to the internet or other external connections.

Remediation:

- On the system where your SharePoint platform is installed, open a command-line window and type the following command:

```
cd %CommonProgramFiles%\Microsoft Shared\Web Server Extensions\12\bin
```

- Determine the current port number for the Central Administration Web site, by typing the following command:

```
stsadm -o getadminport
```

- Configure your firewall so that the SharePoint system and the identified port is not exposed to external connections.

References:

1. https://technet.microsoft.com/en-us/library/cc262849.aspx
2. https://technet.microsoft.com/en-us/library/cc288247(v=office.12).aspx

CIS Controls:

9.4 Ensure Only Necessary Servers Are Internet-exposed
Verify any server that is visible from the Internet or an untrusted network, and if it is not required for business purposes, move it to an internal VLAN and give it a private address.

2.10 Ensure Dbcreator and Securityadmin roles are only used as needed (Scored)

Profile Applicability:

- Level 1

Description:

In certain situations, database administrators (DBAs) may want to operate independently from SharePoint 2016 administrators and create and manage all the databases. This is typical in IT environments where security requirements and company policies require a separation of administrator roles. The farm administrator provides SharePoint 2016 database requirements to the DBA, who then creates the necessary databases and sets up the logins that are required for the farm.

Rationale:

The ability to grant access to the database engine and to configure user permissions allows the securityadmin to assign most server permissions. You should treat the securityadmin role as equal to the sysadmin role.

Audit:

Using `SQL Server Management Studio` access `Object Explorer`.

1. Expand the server in which you want to view a `fixed server role`.
2. Expand the `Security` folder.
3. Expand the `Server Roles` folder.
4. Right-click the `dbcreator` or `securityadmin` role and select `Properties`.
5. In the `dbcreator` or `securityadmin` dialog box, on the `Members` page view the list of members.

Remediation:

Using `SQL Server Management Studio` access `Object Explorer`.

1. Expand the server in which you want to view a `fixed server role`.
2. Expand the `Security` folder.
3. Expand the `Server Roles` folder.
4. Right-click the `dbcreator` or `securityadmin` role and select `Properties`.
5. In the `dbcreator` or `securityadmin` dialog box, on the `Members` page click the list of members.
6. Remove the members from the list.

References:

1. https://technet.microsoft.com/en-us/library/hh377944.aspx

CIS Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

2.11 Ensure that the SharePoint Online Web Part Gallery component is configured with limited access (Scored)

Profile Applicability:

- Level 1

Description:

For each SharePoint web application, the platform should be configured to prevent users from accessing the Online Web Part Gallery.

Rationale:

Web parts are reusable components that render sections of a SharePoint Web page. The available web parts are displayed in the Web Parts Gallery, which is a collection of web parts located on the internet. The Online Gallery could contain Web Parts from unknown third parties, which could increase the risk of a malicious code execution attack. Preventing users from accessing the Online Web Part Gallery decreases the system's attack surface.

Audit:

Log in to Central Administration.
Navigate to `Security > Manage Web Part Security`
For each web application in the Web Application section perform the following:

- Select the correct web application in the Web Application section.
- Verify the "Prevents users from accessing the Online Web Part Gallery, and helps to improve security and performance" option is checked.

Remediation:

Login to Central Administration.
Navigate to `Security > Manage Web Part Security`
For each web application in the web application section, perform the following:

- Select the correct web application in the web application section.
- Select the "Prevents users from accessing the Online Web Part Gallery, and helps to improve security and performance" option in the Online Web Part Gallery section.

References:

1. https://social.technet.microsoft.com/wiki/contents/articles/37543.sharepoint-2016-central-admin-security-manage-web-part-security.aspx

CIS Controls:

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

3 Secure Infrastructure Design

3.1 Ensure a secondary SharePoint site collection administrator has been defined on each site collection. (Scored)

Profile Applicability:

- Level 1

Description:

A secondary SharePoint site collection administrator must be defined when creating a new site collection.

Rationale:

If a site reaches its maximum size, users will be denied access until an administrator fixes the problem. Having a secondary administrator reduces the risk of having a Denial-of-Service on a site. If the site reaches its maximum size, the secondary administrator can fix the problem if the primary administrator is not available. In some situations, having a secondary site administrator could be inappropriate for reasons of control or confidentiality.

Audit:

1. Log on to `SharePoint Central Administration` as a member of the Farm Administration Group.
2. Click on `Application Management`.
3. Select `Site Collections > Change Site Collections Administrator`.
4. For each site, verify if a Secondary Site Collection Administrator has been defined.

Remediation:

1. Log on to `SharePoint Central Administration` as a member of the Farm Administration Group.
2. In `Central Administration`, click `Application Management`.
3. On the `Site Collection Administrators` page, click the arrow next to the site collection name, and then select `Change Site Collection` if the site collection you want is not already selected.
4. Select the URL of the site collection, and then click `OK`. If the site collection is not listed, click the arrow next to the web application name, click `Change Web Application`, select the name of the web application that contains the site collection, select the URL of the site collection, and then click `OK`.

5. In the secondary site collection administrator area, either type the name of the user whom you want to add by using the format `<domain>\<username>` or select the user by using the address book.
6. Click `OK`

References:

1. https://technet.microsoft.com/en-us/library/ff631156(v=office.16).aspx#section1

CIS Controls:

5 Controlled Use of Administration Privileges
Controlled Use of Administration Privileges

3.2 Ensure SharePoint implements an information system isolation boundary that minimizes the number of non-security functions included within the boundary containing security functions. (Not Scored)

Profile Applicability:

- Level 1

Description:

Review the SharePoint server configuration to ensure an information system isolation boundary that minimizes the number of non-security functions included within the boundary containing security functions are implemented.

Rationale:

The information system isolates security functions from non-security functions by means of an isolation boundary (implemented via partitions and domains) controlling access to and protecting the integrity of, the hardware, software, and firmware that perform those security functions. The information system maintains a separate execution domain (e.g., address space) for each executing process.

Audit:

1. Log on to the server that hosts the farm's Central Administration website.
2. Open `IIS Manager`.
3. Expand `Sites` tree view and right-click the web application named `SharePoint Central Administration`.
4. Select `Edit Bindings ....`
5. Confirm the site is bound to an out-of-band (OOB) or non-production IP address.

Remediation:

1. In the server hosting the farm's Central Administration website Open 'IIS Manager'.
2. Expand `Sites` tree view and right-click the web application named `SharePoint Central Administration`.
3. Select `Edit Bindings ....`
4. Change the site is bound to an out-of-band (OOB) IP address.

CIS Controls:

11.7 Manage Network Infrastructure Using Segregation
Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

3.3 Ensure SharePoint implements security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers. (Not Scored)

Profile Applicability:

- Level 1

Description:

SharePoint must implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.

Rationale:

The information system isolates security functions from nonsecurity functions by means of an isolation boundary (implemented via partitions and domains) controlling access to, and protecting the integrity of, the hardware, software, and firmware that perform those security functions. The information system maintains a separate execution domain (e.g., address space) for each executing process.

Audit:

Review the SharePoint server configuration to ensure security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers are implemented.

1. Check the network location of the Central Administration server.

If the server resides in the DMZ, this is a finding.

2. Attempt to access Central Administration without first connecting to a management network VPN.

If Central Administration can be accessed over a production network, this is a finding.

3. Attempt to connect directly to a SharePoint server (i.e., via remote desktop) without first connecting to a management network VPN.

If a remote desktop session can be established via a production network, this is a finding.

Remediation:

Move Central Administration servers to an isolated section of the network.

CIS Controls:

11.7 Manage Network Infrastructure Using Segregation
Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

3.4 Ensure SharePoint identifies data type, specification, and usage when transferring information between different security domains so policy restrictions may be applied. (Not Scored)

Profile Applicability:

- Level 1

Description:

SharePoint must identify data type, specification, and usage when transferring information between different security domains so policy restrictions may be applied.

Rationale:

Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information.

Flow control is based on the characteristics of the information and/or the information path. Applications providing flow control must identify data type, specification, and usage when transferring information between different security domains so policy restrictions may be applied.

A security domain is defined as a domain implementing a security policy and administered by a single authority.

Data type, specification, and usage includes using file naming to reflect the type of data being transferred and limiting data transfer based on file type.

Audit:

Review the SharePoint server configuration to ensure data type, specification, and usage when transferring information between different security domains are identified so policy restrictions may be applied.
An IRM must be enabled in SharePoint. The Windows Rights Management Services (RMS) (or a comparable IRM product) can either be located through Active Directory or specified.

1. In `Central Administration`, click on `Security`.
2. On the `Security` page, in the Information policy list, click `Configure information rights management`.

If `Do not use IRM on this server` is selected, or if a configuration error message is displayed (such as `... IRM will not work until the client is configured properly`), this is a finding.

Remediation:

1. In `Central Administration`, click on `Security`.
2. On the `Security` page, in the Information policy list, click `Configure information rights management`.
3. Ensure `Do not use IRM on this server` is not selected.

CIS Controls:

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

3.5 Ensure that SharePoint specific malware (i.e. anti-virus) protection software is integrated and configured (Scored)

Profile Applicability:

- Level 1

Description:

SharePoint-specific malware (i.e. anti-virus) protection software must be integrated and configured.

Rationale:

Configuring anti-virus settings ensures documents will be scanned for viruses upon download from and upload to the SharePoint server. Anti-virus settings are not configured by default, therefore leaving the documents downloaded from or uploaded to SharePoint open to potential malware.

Audit:

1. Log on to the `Central Administration` website.
2. Navigate to `Operations > Security Configuration`.
3. Select `Anti-virus`. Validate each of the following boxes are selected:
    - Scan documents on upload.
    - Scan documents on download.
    - Attempt to clean infected documents.

Remediation:

1. Log on to the `Central Administration` website.
2. Navigate to `Operations > Security Configuration`.
3. Select `Anti-virus`.
4. SharePoint specific malware (i.e. anti-virus) protection software must be integrated and configured for each of the following:
    - Scan documents on upload.
    - Scan documents on download.
    - Attempt to clean infected documents.

CIS Controls:

8.1 Deploy Automated Endpoint Protection Tools
Employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality.

All malware detection events should be sent to enterprise anti-malware administration tools and event log servers.

3.6 Ensure that SharePoint is configured with "Strict" browser file handling settings (Scored)

Profile Applicability:

- Level 1

Description:

SharePoint must prevent the execution of prohibited mobile code.

Rationale:

Decisions regarding the utilization of mobile code within organizational information systems need to include evaluations that help determine the potential for the code to cause damage to the system if used maliciously.

Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations.

Applications can prevent the execution of prohibited mobile code by leveraging architectures that provide a virtual execution environment sometimes referred to as a "sandbox". The mobile code is executed within this isolated environment apart from the host's indigenous operating environment that allows for mobile code capability restrictions and helps to prevent malicious code from accessing system resources and data.

The application must prevent the execution of prohibited mobile code.

Audit:

1. Navigate to `Central Administration` website.
2. Click `Manage Web Applications`.
3. For each Web Application in the Farm:

   - Click on the `Web Application` to configure.
   - Click on the drop-down box below `General Settings`.
   - Click on `General Settings` in the drop down box.
   - Under `Browser File Handling`, verify that `Strict` is selected.

Remediation:

1. Navigate to `Central Administration` website.
2. Click `Manage Web Applications`.
3. For each Web Application in the Farm:

    - Click on the `Web Application` to configure.
    - Click on the drop-down box below `General Settings`.
    - Click on `General Settings` in the drop down box.
    - Under `Browser File Handling`, select `Strict`.

CIS Controls:

2 Inventory of Authorized and Unauthorized Software
Inventory of Authorized and Unauthorized Software

3.7 Ensure that SharePoint is set to reject or delay network traffic generated above configurable traffic volume thresholds. (Not Scored)

Profile Applicability:

- Level 1

Description:

SharePoint must reject or delay, as defined by the organization, network traffic generated above configurable traffic volume thresholds.

Rationale:

It is critical when a system is at risk of failing to process audit logs as required; actions are automatically taken to mitigate the failure or risk of failure.

One method used to thwart the auditing system is for an attacker to attempt to overwhelm the auditing system with large amounts of irrelevant data. Consequently, either audit logs are being overwritten or disk space is being exhausted. In such cases, activity is either being erased from the logs or not recorded at all due to the lack of disk space.

In many system configurations, the disk space allocated to the auditing system is separate from the disks allocated for the operating system; therefore, this may not result in a system outage.

Audit:

Access the `Internet Information Service Manager` on the appropriate SharePoint server.

1. For each site `IIS site` subject to user traffic, select the `site`.
2. Click `Advanced Settings`.
3. Expand `Connection Limits`.
4. Ensure the following settings possess a value:

    - `Connection Time-Out`
    - `Maximum Bandwidth`
    - `Maximum Concurrent Connections`

5. Repeat steps for each site subject to user traffic.

Remediation:

Access the `Internet Information Service Manager` on the appropriate SharePoint server.

1. For each site `IIS site` subject to user traffic, select the `site`.
2. Click `Advanced Settings`.
3. Expand `Connection Limits`.
4. Ensure the following settings possess a value:

    - `Connection Time-Out`
    - `Maximum Bandwidth`
    - `Maximum Concurrent Connections`

5. Repeat steps for each site subject to user traffic.

CIS Controls:

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

3.8 Ensure that On-Premise SharePoint servers is configured without OneDrive redirection linkages. (Scored)

Profile Applicability:

- Level 1

Description:

Disable OneDrive Redirection for On-Premise SharePoint servers

Rationale:

OneDrive Redirection allows users and organizations to redirect their SharePoint sites to the cloud which may potentially increase the risk exposure to any sensitive information.

Audit:

1. Navigate to the `Central Administration` Menu in SharePoint.
2. Click on `Configure OneDrive` and `Site` links.
3. Verify there is no URL in the `My Site URL` field.

Remediation:

1. Navigate to the `Central Administration` Menu in SharePoint.
2. Click on `Configure OneDrive` and `Site` links.
3. Remove any URLs in the `My Site URL` field.

CIS Controls:

13 Data Protection
Data Protection

3.9 Ensure that the default SharePoint database server ports are changed and/or disabled (Not Scored)

Profile Applicability:

- Level 1

Description:

Default ports for SharePoint database servers should be changed and/or disabled.

Rationale:

Default database ports provide a malicious actor with the ability to identify and connect to database services. Changing the default ports reduces the risk exposure.

Audit:

Verify the database port current used is not a default port by connecting to that port.

Remediation:

Change the default database connectivity port and implement firewall rules to block default ports.

Default Value:

1433

CIS Controls:

12 Boundary Defense
Boundary Defense

3.10 Ensure that SharePoint application servers are protected by a reverse proxy (Not Scored)

Profile Applicability:

- Level 1

Description:

A reverse proxy is server component that sits between the internet and the web servers. It accepts HTTP requests, provides various services, and forwards the requests to one or many servers.

Rationale:

Having a point at which one can inspect, transform and route HTTP requests before they reach the SharePoint web servers provides significant benefits. A reverse proxy can hide the topology and characteristics of the back-end SharePoint servers by removing the need for direct internet access. A reverse proxy can be placed in an internet facing DMZ, and hide the SharePoint web servers inside a non-public subnet.

Audit:

Review the SharePoint server architecture and determine if all HTTP requests are routed through a reverse proxy.

Remediation:

Implement a reverse proxy to process all HTTP requests and route them to the SharePoint servers.

Impact:

A malicious attacker can directly attack a SharePoint server that is placed in the DMZ.

References:

1. https://technet.microsoft.com/en-us/library/dn607304.aspx

CIS Controls:

12 Boundary Defense
Boundary Defense

3.11 Ensure SharePoint database servers are segregated from application server and placed in a secure zone. (Not Scored)

Profile Applicability:

- Level 1

Description:

Segregating the SharePoint database server from the application server provides a layered defense architecture.

Rationale:

A layered defense architecture provides additional security and reduces the attack vector of an environment. When the SharePoint database server is segregated from the application server only specific ports can be opened from the application server to the database server reducing the attack vector and access to the critical data stored on the SharePoint database.

Audit:

Review the SharePoint server architecture and identify if the SharePoint database server is segregated and placed in a secure network zone.

Remediation:

Review the SharePoint server architecture and move the SharePoint database server in a secure network zone. Only open the specific ports required from the application server to the database server.

Impact:

A malicious actor could gain access to the SharePoint database server and extract the sensitive information stored in the database.

References:

1. https://technet.microsoft.com/en-us/library/hh292622.aspx

CIS Controls:

9.5 Operate Critical Services On Dedicated Hosts (i.e. DNS, Mail, Web, Database)
Operate critical services on separate physical or logical host machines, such as DNS, file, mail, web, and database servers.

3.12 Ensure that the SharePoint Central Administration interface is not hosted in the DMZ. (Scored)

Profile Applicability:

- Level 1

Description:

The SharePoint Central Administration site should not be installed onto the network DMZ, which is exposed to external internet connections.

Rationale:

SharePoint installed Central Administrator is a powerful management tool used to administer the farm. This server should be installed on a trusted network segment. This server should also be used to run services rather than user-oriented web applications.

Audit:

On an administrative workstation, open `Central Administration` and make note of the URL (i.e., http://sharepointserver:7040).
Try to open the `Central Administration application` on a workstation or server in the DMZ by opening a Web browser and type in the URL to `Central Administration`.

Remediation:

For environments requiring an Internet-facing capability, remove the SharePoint Central Administration application server upon which Central Administration is installed from the DMZ.
On the existing farm remove the `Central Administration website` by:

1. Run the `SharePoint configuration wizard`.
2. Select `Do not disconnect from the server farm`.
3. Select `Yes, I want to remove the website from this machine`.
4. Select `OK`.

CIS Controls:

12 Boundary Defense
Boundary Defense

4 Authentication

4.1 Ensure SharePoint displays an approved system use notification message or banner before granting access to the system. (Scored)

Profile Applicability:

- Level 1

Description:

SharePoint web applications must display an approved system use notification message or banner before granting access.

Rationale:

Applications are required to display an approved system use notification message or banner before granting access to the system providing privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Audit:

Verify that a banner occurs on a per-Web Application basis:

1. Obtain a listing of all `SharePoint Web applications`.
2. Open a Web browser and navigate to the `SharePoint Web application home page`.
3. Verify the authorized warning banner text is displayed.

Remediation:

Configure all SharePoint web applications to display the authorized warning banner text at session start. There are many ways to ensure that a warning banner text is shown to the user when using the web application. The following is only one such method of doing so. For each existing SharePoint site or web application:

1. Verify that a `global.asax` file exists in each SharePoint web application root directory.
2. Create a back-up on the `global.asax` file in a safe location.
3. Create a banner page resource file within the web application directories, created to display the authorized warning banner text and redirects the user back to the web application afterwards.

4. Modify the web application global.asax file to add a `Session_Start` method that redirects the user to the banner page resource created from step 3.

The created banner page resource should successfully display the banner upon the start of a new session and redirect the user to the web application afterwards.

CIS Controls:

16 Account Monitoring and Control
Account Monitoring and Control

4.2 Ensure claims-based authentication is used for all web applications and zones of a SharePoint 2016 farm (Scored)

Profile Applicability:

- Level 1

Description:

Claims-based authentication enables systems and applications to authenticate a user without requiring the user to disclose more personal information than necessary. SharePoint continues to offer support for both claims and classic authentication modes. Claims-based identity is an identity model in SharePoint that includes features such as authentication across users of Windows-based systems and systems that are not Windows-based, multiple authentication types, stronger real-time authentication, a wider set of principal types, and delegation of user identity between applications.

When a user signs in to SharePoint, the user's token is validated and then used to sign in to SharePoint. The user's token is a security token issued by a claims provider. When you build claims-aware applications, the user presents an identity to the application as a set of claims. One claim could be the user's name, another might be an email address. The external identity system is configured to give your application all the information that it needs about the user with each request, along with cryptographic assurance that the identity data received by the application comes from a trusted source.

Rationale:

Claims-based identity allows you to factor out the authentication logic from individual applications. Instead of the application determining who the user is, it receives claims that identify the user.

In software, this bundle of claims is called a security token. Each security token is signed by the issuer who created it. A claims-based application considers users to be authenticated if they present a valid, signed security token from a trusted issuer which is a lot more secure than classic authentication.

Audit:

1. Navigate to `Central Administration website`.
2. Click on `Manage web applications`.
3. Click on the site you're planning to verify `Claims Based Authentication`.
4. Under `Web Applications` tab click on the `Authentication Providers icon`.

5. Under the small window pop-up verify if the `default value` is set to `Claims Based Authentication`.

Remediation:

1. Navigate to `Central Administration website`.
2. Click on `Manage web applications`.
3. Click on the site you're planning to verify `Claims Based Authentication`.
4. Under `Web Applications` tab click on the `Authentication Providers icon`.
5. Under the small window pop-up verify if the `default value` is set to `Windows`.
6. Create a PowerShell (.ps1) file and paste the following code into it:
   ```
   $setcba = Get-SPWebApplication "http://<YourSiteURL>"
   $setcba.UseClaimsAuthentication = 1;
   $setcba.Update()
   ```
7. Save the Code as `SetClaimsBasedAuthentication.ps1` on the SharePoint server.
8. Execute the PowerShell script from the `SharePoint Management Shell` using the following command `./SetClaimsBasedAuthentication.ps1`

Default Value:

Default value is set to Windows.

References:

1. https://technet.microsoft.com/en-us/library/cc262350(v=office.16).aspx

CIS Controls:

16.9 Configure Account Access Centrally
Configure access for all accounts through a centralized point of authentication, for example Active Directory or LDAP. Configure network and security devices for centralized authentication as well.

4.3 Ensure Windows Authentication uses Kerberos and not the NT Lan Manager (NTLM) authentication protocol (Not Scored)

Profile Applicability:

- Level 1

Description:

If Windows Authentication mechanisms are used on SharePoint, the system should be configured to use the Kerberos authentication protocol rather than the NT Lan Manager (NTLM) equivalent.

Rationale:

There are a few factors in which Kerberos is superior to NTLM authentication and is indeed preferred. First, Kerberos offers faster authentication because it does not require multiple servers and components to complete authentication tasks, as in the case of NTLM authentication. Second, Kerberos offers mutual authentication. Kerberos can authenticate the client to the server and importantly, also the server to the client.

Audit:

1. Launch `Central Administration`.
2. Click on `Application Management` then `Manage web applications`.
3. In `Authentication Providers` click each available zone.
4. Under `Authentication Providers - Zone popup` verify `Integrated Windows authentication`
   is checked and `Negotiate (Kerberos)` is selected.

Remediation:

1. Launch `Central Administration`.
2. Click on `Application Management` then `Manage web applications`.
3. In `Authentication Providers` click each available zone.
4. Under `Authentication Providers - Zone popup` check `Integrated Windows authentication`
   and select `Negotiate (Kerberos)`.

CIS Controls:

16.9 Configure Account Access Centrally
Configure access for all accounts through a centralized point of authentication, for example

Active Directory or LDAP. Configure network and security devices for centralized authentication as well.

4.4 Ensure Anonymous authentication is denied (Not Scored)

Profile Applicability:

- Level 1

Description:

SharePoint web applications should be configured to disallow anonymous authentication, which would allow users to authenticate and use the applications without confirming their identity.

Rationale:

Allowing anonymous authentication to SharePoint web applications will nullify the effectiveness of the authentication control. Furthermore, any activity performed in the anonymous session would also not be linkable to a particular account. Such linkages are often critical in post-incident investigations and audits.

Audit:

1. Navigate to `Central Administration` website.
2. Click on `Manage web applications`.
3. Click the web application name.
4. Click the `Authentication Providers` button in the `Web Applications` ribbon.
5. Click each Zone, and verify that the `Enable anonymous access` check box is not selected.
6. Repeat for each web application.

Remediation:

1. Navigate to `Central Administration` website.
2. Click on `Manage web applications`.
3. Click the web application name.
4. Click the `Authentication Providers` button in the `Web Applications` ribbon.
5. Click each Zone, and uncheck `Enable anonymous access`.
6. Repeat for each web application.

CIS Controls:

16 <u>Account Monitoring and Control</u>
Account Monitoring and Control

5 Auditing

5.1 Ensure that auditable events and diagnostic tracking settings within the SharePoint system is consistent with the organization's security plans (Scored)

Profile Applicability:

- Level 1

Description:

SharePoint must allow designated organizational personnel to select which auditable events are to be audited by specific components of the system.

Rationale:

Audit records can be generated from various components within the information system, such as network interfaces, hard disks, modems, etc. From an application perspective, certain specific application functionalities may be audited as well.

The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating audit records (i.e., auditable events, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked).

Organizations may define the organizational personnel accountable for determining which application components shall provide auditable events.

Audit:

Navigate to `Central Administration`.

1. Click `Monitoring`.
2. Click `Configure Diagnostic Logging`.

Validate that the selected `event categories` and `trace levels` match those defined by the organization's system security plan.
If the selected event categories/trace levels are inconsistent with those defined in the organization's system security plan, this is a finding.

Remediation:

Navigate to `Central Administration`.

1. Click `Monitoring`.
2. Click `Configure Diagnostic Logging`.

Configure the `event categories` and `trace levels` to match those defined by the organization's system security plan.

CIS Controls:

6 Maintenance, Monitoring, and Analysis of Audit Logs
Maintenance, Monitoring, and Analysis of Audit Logs

5.2 Ensure that remote sessions for accessing security functions and security-relevant information are audited (Not Scored)

Profile Applicability:

- Level 1

Description:

Remote access to SharePoint security functions (e.g., user management, audit log management, etc.) and security relevant information requires the activity be audited by the organization.

Rationale:

Any remote administrative or security related access to the SharePoint farm must be audited in order to track system activity, assist in diagnosing system issues and provide evidence needed for forensic investigations post security incident. It is also important to verify and validate the security controls that are in place on the platform.

Audit:

To verify audit settings at the site collection level for each site collection level subject to auditing per organizational requirements:
Navigate to `Site Collection Administration`:

1. Click on `Settings`.
2. Click on `Site Settings`.
3. Click `Site collection audit settings`.
4. Verify the events that are required to audit are selected.
5. Click `OK`.

Remediation:

To configure audit settings at the site collection level for each site collection level subject to auditing per organizational requirements:
Navigate to `Site Collection Administration`:

1. Click on `Settings`.
2. Click on `Site Settings`.
3. Click `Site collection audit settings`.
4. Select the events that are required to be audited.
5. Click `OK`.

CIS Controls:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

6 Services and Connections

6.1 Ensure that the SQL Server component to SharePoint is set to listen on non-default ports, with the defaults (UDP 1434 and TCP 1433) disabled (Scored)

Profile Applicability:

- Level 1

Description:

The default instance of SQL Server listens for client requests on TCP 1433. By default, client computers that connect to SQL Server first connect by using TCP 1433. If this communication is unsuccessful, the client computers query the SQL Server Resolution Service that is listening on UDP 1434 to determine the port on which the database instance is listening.

Rationale:

The default port-communication behavior of SQL Server introduces several issues that affect server hardening. First, the ports used by SQL Server are well-publicized ports and the SQL Server Resolution Service has been the target of buffer overrun attacks and denial-of-service attacks, including the "Slammer" worm virus. Even if SQL Server is updated to mitigate security issues in the SQL Server Resolution Service, the well-publicized ports remain a target. Second, if databases are installed on a named instance of SQL Server, the corresponding communication port is randomly assigned and can change. This behavior can potentially prevent server-to-server communication in a hardened environment.

Audit:

1. Verify that the `User account` that is performing this procedure is a member of either the `sysadmin` or the `serveradmin` fixed server role.
2. Navigate to `SQL Server Configuration Manager` on the computer that is running `SQL Server`.
3. Expand `SQL Server Network Configuration` in the navigation pane.
4. Click the corresponding entry for the instance that you are examining. The default instance is listed as `Protocols for MSSQLSERVER`. Named instances will appear as `Protocols for named_instance`.
5. Right-click `TCP/IP` in the main window in the `Protocol Name` column,
6. Click on `Properties`.

7. Click on the `IP Addresses` tab.
   For every IP address that is assigned to the computer that is running SQL Server, there is a corresponding entry on this tab. By default, SQL Server listens on all IP addresses that are assigned to the computer.

To globally examine the port that the default instance is listening on, follow these steps:

1. For each `IP address` except `IPAll`, examine all values for both `TCP dynamic ports` and `TCP Port`.
2. For `IPAll`, examine the value for `TCP dynamic ports`.

To globally examine the port that a named instance is listening on, follow these steps:

1. For each IP address including `IPAll`, examine all values for `TCP dynamic ports`. A value of `0` for this field indicates that SQL Server uses a dynamic TCP port for the IP address. A `blank entry` for this value means that SQL Server will not use a dynamic TCP port for the IP address.

Remediation:

1. Verify that the `User account` that is performing this procedure is a member of either the `sysadmin` or the `serveradmin` fixed server role.
2. Navigate to `SQL Server Configuration Manager` on the computer that is running `SQL Server`.
3. Expand `SQL Server Network Configuration` in the navigation pane.
4. Click the corresponding entry for the instance that you are examining. The default instance is listed as `Protocols for MSSQLSERVER`. Named instances will appear as `Protocols for named_instance`.
5. Right-click `TCP/IP` in the main window in the `Protocol Name` column,
6. Click on `Properties`.
7. Click on the `IP Addresses` tab.
   For every IP address that is assigned to the computer that is running SQL Server, there is a corresponding entry on this tab. By default, SQL Server listens on all IP addresses that are assigned to the computer.

To globally examine the port that the default instance is listening on, follow these steps:

1. For each `IP address` except `IPAll`, examine all values for both `TCP dynamic ports` and `TCP Port` and confirm UDP 1434 and TCP 1433 are blocked.
2. For `IPAll`, examine the value for `TCP dynamic ports` and confirm UDP 1434 and TCP 1433 are blocked.

Default Value:

No ports are blocked.

References:

1. https://technet.microsoft.com/en-us/library/cc262849.aspx

CIS Controls:

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

6.2 Ensure HTTPS binding: TCP 32844 is used (Scored)

Profile Applicability:

- Level 1

Description:

By default, communication between Web servers and service applications within a farm takes place by using HTTP with a binding to TCP 32843.

Rationale:

Forcing communication over HTTPS TCP 32844 hardens the communication between service applications.

Audit:

On the Service Applications page in Central Administration, view setting for the service application.

Remediation:

On the Service Applications page in Central Administration, select the service application, and then click Publish.

References:

1. https://technet.microsoft.com/en-us/library/cc262849.aspx

CIS Controls:

9 Limitation and Control of Network Ports, Protocols, and Services
Limitation and Control of Network Ports, Protocols, and Services

14.2 Encrypt All Sensitive Information Over Less-trusted Networks
All communication of sensitive information over less-trusted networks should be encrypted. Whenever information flows over a network with a lower trust level, the information should be encrypted.

6.3 Ensure that SharePoint user sessions are terminated upon user logoff and when the idle time limit is exceeded (Not Scored)

Profile Applicability:

- Level 1

Description:

The SharePoint platform should be configured with a user session idle time limit of 15 minutes.

Rationale:

Whenever a SharePoint user sessions is started, a unique session ID and other session information are generated. Such information can be used be a malicious user to hijack the session. By terminating sessions upon user logoff and idle time limit, the underlying session information is invalidated. Therefore, the potential for the session to be hijacked is removed.

Audit:

Review the SharePoint server configuration to ensure user sessions are terminated upon user logoff, and when idle time limit is exceeded.
Navigate to Central Administration website.
Click `Application Management`.
Click `Manage Web Applications`.
Repeat the following steps for each web application:

- Select the `Web Application`.
- Click `General Settings` in the `Web Application` ribbon.
- In the `Web Page Security Validation` section, verify that `Security Validation` is: is
  set to `On` and that the `Security Validation Expires`: setting is set to `15 minutes`.

Remediation:

Review the SharePoint server configuration to ensure user sessions are terminated upon user logoff, and when idle time limit is exceeded.
Navigate to Central Administration website.
Click `Application Management`.
Click `Manage Web Applications`.
Repeat the following steps for each web application:

- Select the `Web Application`.
- Click `General Settings` in the `Web Application` ribbon.
- In the `Web Page Security Validation` section, verify that `Security Validation` is: is set to `On` and that the `Security Validation Expires`: setting is set to `15 minutes`

CIS Controls:

3.1 Establish Standard Secure Configurations For OS And Software
Establish standard secure configurations of operating systems and software applications. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.

7 Web.Config Configuration

7.1 Ensure that the MaxZoneParts setting for Web Part limits is set to 100. (Scored)

Profile Applicability:

- Level 1

Description:

Limit the number of web parts in SharePoint to 100.

Rationale:

A user can create too many personal views. With personal views, SharePoint actually adds each view as a web part on the page. If a user has 10 personal views, there are actually 10 web parts on the page. 9 of those web parts are hidden depending on the personal view selected. When SharePoint reaches the default maximum of 50 web parts on the page, it will throw an error.

Audit:

Navigate to the `IIS Manager` on the Web Front End (WFE) servers

1. Click on the `Sites` folder.
2. Highlight the `site (web application)`.
3. On the right-hand navigation bar, Click on `Explore`.
4. Open the `web.config` file with Notepad.
5. Find the following phrase: `<WebPartLimits MaxZoneParts="50" PropertySize="1048576"/>`.
6. Verify the value for `MaxZoneParts` is set to 100.
7. Repeat for the remaining Web Front End servers.

Remediation:

Navigate to the `IIS Manager` on the Web Front End (WFE) servers

1. Click on the `Sites` folder.
2. Highlight the `site (web application)`.
3. On the right-hand navigation bar, Click on `Explore`.
4. Open the `web.config` file with Notepad.

5. Find the following phrase: `<WebPartLimits MaxZoneParts="50" PropertySize="1048576"/>`.
6. Change the value for `MaxZoneParts` from 50 to 100.
7. Save the file.
8. Open a command prompt as Administrator and type in `iisreset` to restart IIS.
9. Repeat for the remaining Web Front End servers.

Impact:

SharePoint will throw errors if the number of web parts is not limited.

Default Value:

50 web parts per page

References:

1. https://technet.microsoft.com/en-us/library/cc262849(v=office.16).aspx

CIS Controls:

18 Application Software Security
Application Software Security

7.2 Ensure that the SafeControls list is set to the minimum set of controls needed for your sites (Scored)

Profile Applicability:

- Level 1

Description:

The Safe Controls list contains the names of controls and Web Parts, specific to your SharePoint site, that server administrators can designate as safe for use on any .aspx page within a site. This list is part of the Web.config file in your Web application root.

Rationale:

A fundamental assumption of the Windows SharePoint Services technology is that "untrusted users" can upload and create ASPX pages within the system on which Windows SharePoint Services is running. These users should be prevented from adding server-side code within ASPX pages, but there should be a list of approved controls that those untrusted users can use. One way to provide these controls is to create a Safe Controls list.

Audit:

1. Locate the `Web.config` file in your application root directory and open it.
2. Verify the following safe-control entry for your custom assembly to the Web.config file:

```
<SafeControl Assembly="<YourWebPartName>, Version=1.0.0.0, Culture=neutral,
PublicKeyToken=null" Namespace="<YourWebPartNamespace>" TypeName="*"
Safe="True" AllowRemoteDesigner="True"/>
```

`<YourWebPartName>` is the name of the Web Part that is being deployed.

`<YourWebPartNamespace>` is the namespace that is associated with your Web Part.

Remediation:

1. Copy the `<YourWebPartName>.dll` assembly in the project's Bin directory to the Bin directory in your Web application root directory. For example: `C:\inetpub\wwwroot\wss\VirtualDirectories\80\`.
2. Locate the `Web.config` file in your application root directory and open it for editing.
3. Add the following safe-control entry for your custom assembly to the Web.config file:

```
<SafeControl Assembly="<YourWebPartName>, Version=1.0.0.0, Culture=neutral,
PublicKeyToken=null" Namespace="<YourWebPartNamespace>" TypeName="*"
Safe="True" AllowRemoteDesigner="True"/>
```

`<YourWebPartName>` is the name of the Web Part that is being deployed.

`<YourWebPartNamespace>` is the namespace that is associated with your Web Part.

Impact:

Malicious users can upload and create ASPX pages.

References:

1. https://technet.microsoft.com/en-us/library/cc261736.aspx#BKMK_SafeControls

CIS Controls:

18 Application Software Security
Application Software Security

7.3 Ensure compilation or scripting of database pages via the PageParserPaths elements is not allowed (Scored)

Profile Applicability:

- Level 1

Description:

Allowing compilation or scripting of database pages via the "PageParserPaths" elements can lead to disclosure of compilation error messages containing server info and source code exposed to the user.

Rationale:

Audit:

1. Open `Web.config` file
2. Check if the `PageParserPath` parameter is set with a value which includes `*` or any folder/webpage in the application:

```
<PageParserPaths>
    <PageParserPath VirtualPath="*" CompilationMode="Always"
              AllowServerSideScript="true" IncludeSubFolders="true" />
</PageParserPaths>
```

Remediation:

Do not allow compilation or scripting of database pages via the PageParserPaths elements in Web.Config file

Impact:

Information Disclosure of server path, Operating system info and source code to the user by compilation error messages.

Default Value:

By default, the tag in application wab.config file is empty.

References:

1. https://technet.microsoft.com/en-us/library/cc262849(v=office.16).aspx

2. https://msdn.microsoft.com/en-us/library/bb964680(v=office.12).aspx

CIS Controls:

18 Application Software Security
Application Software Security

7.4 Ensure the SharePoint CallStack and AllowPageLevelTrace "SafeMode" parameters are set to false (Scored)

Profile Applicability:

- Level 1

Description:

The CallStack and PageLevelTrace parameters are used when debugging a problem and displays detailed additional information.

Rationale:

The detailed additional information provided by the CallStack and PageLevelTrace parameters can be used by a malicious actor to gain sensitive information about the system parameters and application.

Audit:

Locate the `Web.config`file in your application root directory and open it.
Verify the following `SafeMode` entry in the `Web.config` file:

1. Verify parameter `CallStack="false"`.
2. Verify parameter `AllowPageLevelTrace="false"`.
3. Close the `Web.config` file without saving it.

Remediation:

Locate the `Web.config`file in your application root directory and edit it.
Edit the following `SafeMode` entry in the `Web.config` file:

1. Edit parameter `CallStack="false"`.
2. Edit parameter `AllowPageLevelTrace="false"`.
3. Close the `Web.config` file and save it.

Impact:

System sensitive information can be compromised.

References:

1. https://technet.microsoft.com/en-us/library/cc262849(v=office.16).aspx

CIS Controls:

18.5 Sanitize Output Of Applications
Do not display system error messages to end-users (output sanitization).

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	**Settings**		
1.1	Ensure access to SharePointEmailws.asmx is limited to only the server farm account (Not Scored)	☐	☐
1.2	Ensure that the SharePoint Central Administration Site is TLS-enabled (Not Scored)	☐	☐
1.3	Ensure specific whitelisted IP addresses, IP address ranges, and/or domains are set (Not Scored)	☐	☐
1.4	Ensure that the underlying Internet Information Services (IIS) Authentication module is set to use Kerberos as its Authentication Provider (Not Scored)	☐	☐
2	**Access and Permissions**		
2.1	Ensure 'Block File Types' is configured to match the enterprise blacklist (Scored)	☐	☐
2.2	Ensure the SharePoint farm service account (database access account) is configured with the minimum privileges for the local server. (Scored)	☐	☐
2.3	Ensure the SharePoint setup account is configured with the minimum privileges in Active Directory. (Not Scored)	☐	☐
2.4	Ensure SharePoint provides the ability to prohibit the transfer of unsanctioned information in accordance with security policy. (Not Scored)	☐	☐
2.5	Ensure the SharePoint setup account is configured with the minimum privileges on the SQL server. (Scored)	☐	☐
2.6	Ensure the SharePoint farm service account (database access account) is configured with the minimum privileges on the SQL server. (Scored)	☐	☐
2.7	Ensure only the server farm account has access to SharePointEmailws.asmx (Scored)	☐	☐
2.8	Ensure a separate organizational unit (OU) in Active Directory exists for SharePoint 2016 objects. (Scored)	☐	☐
2.9	Ensure the SharePoint Central Administration site is not accessible from Extranet or Internet connections (Scored)	☐	☐
2.10	Ensure Dbcreator and Securityadmin roles are only used as needed (Scored)	☐	☐
2.11	Ensure that the SharePoint Online Web Part Gallery component is configured with limited access (Scored)	☐	☐
3	**Secure Infrastructure Design**		
3.1	Ensure a secondary SharePoint site collection administrator	☐	☐

	has been defined on each site collection. (Scored)		
3.2	Ensure SharePoint implements an information system isolation boundary that minimizes the number of non-security functions included within the boundary containing security functions. (Not Scored)	□	□
3.3	Ensure SharePoint implements security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers. (Not Scored)	□	□
3.4	Ensure SharePoint identifies data type, specification, and usage when transferring information between different security domains so policy restrictions may be applied. (Not Scored)	□	□
3.5	Ensure that SharePoint specific malware (i.e. anti-virus) protection software is integrated and configured (Scored)	□	□
3.6	Ensure that SharePoint is configured with "Strict" browser file handling settings (Scored)	□	□
3.7	Ensure that SharePoint is set to reject or delay network traffic generated above configurable traffic volume thresholds. (Not Scored)	□	□
3.8	Ensure that On-Premise SharePoint servers is configured without OneDrive redirection linkages. (Scored)	□	□
3.9	Ensure that the default SharePoint database server ports are changed and/or disabled (Not Scored)	□	□
3.10	Ensure that SharePoint application servers are protected by a reverse proxy (Not Scored)	□	□
3.11	Ensure SharePoint database servers are segregated from application server and placed in a secure zone. (Not Scored)	□	□
3.12	Ensure that the SharePoint Central Administration interface is not hosted in the DMZ. (Scored)	□	□
4	**Authentication**		
4.1	Ensure SharePoint displays an approved system use notification message or banner before granting access to the system. (Scored)	□	□
4.2	Ensure claims-based authentication is used for all web applications and zones of a SharePoint 2016 farm (Scored)	□	□
4.3	Ensure Windows Authentication uses Kerberos and not the NT Lan Manager (NTLM) authentication protocol (Not Scored)	□	□
4.4	Ensure Anonymous authentication is denied (Not Scored)	□	□
5	**Auditing**		
5.1	Ensure that auditable events and diagnostic tracking settings within the SharePoint system is consistent with the organization's security plans (Scored)	□	□

5.2	Ensure that remote sessions for accessing security functions and security-relevant information are audited (Not Scored)	□	□
6	**Services and Connections**		
6.1	Ensure that the SQL Server component to SharePoint is set to listen on non-default ports, with the defaults (UDP 1434 and TCP 1433) disabled (Scored)	□	□
6.2	Ensure HTTPS binding: TCP 32844 is used (Scored)	□	□
6.3	Ensure that SharePoint user sessions are terminated upon user logoff and when the idle time limit is exceeded (Not Scored)	□	□
7	**Web.Config Configuration**		
7.1	Ensure that the MaxZoneParts setting for Web Part limits is set to 100. (Scored)	□	□
7.2	Ensure that the SafeControls list is set to the minimum set of controls needed for your sites (Scored)	□	□
7.3	Ensure compilation or scripting of database pages via the PageParserPaths elements is not allowed (Scored)	□	□
7.4	Ensure the SharePoint CallStack and AllowPageLevelTrace "SafeMode" parameters are set to false (Scored)	□	□

Appendix: Change History

Date	Version	Changes for this version
8/17/17	1.0.0	Initial Release