# Information Security Awareness

## WINDOWS SERVER AUDITING

# Acknowledgements

HRD Division

Department of  Electronics and Information Technology

Ministry of Communications and Information Technology

Government of India

## About C-DAC

Centre for Development of Advanced Computing (C-DAC) is the premier R&D organization of the Department of Electronics and Information Technology (DeitY), Ministry of Communications & Information Technology (MCIT) for carrying out R&D in IT, Electronics and associated areas. Different areas of C-DAC, had originated at different times, many of which came out as a result of identification of opportunities.

C-DAC has today emerged as a premier third party R&D organization in IT&E (Information Technologies and Electronics) in the country working on strengthening national technological capabilities in the context of global developments in the field and responding to change in the market need in selected foundation areas. In that process, C-DAC represents a unique facet working in close junction with DeitY to realize nation's policy and pragmatic interventions and initiatives in Information Technology. As an institution for high-end Research and Development (R&D), C-DAC has been at the forefront of the Information Technology (IT) revolution, constantly building capacities in emerging/enabling technologies and innovating and leveraging its expertise, caliber, skill sets to develop and deploy IT products and solutions for different sectors of the economy, as per the mandate of its parent, the Department of Electronics and Information Technology, Ministry of Communications and Information Technology, Government of India and other stakeholders including funding agencies, collaborators, users and the market-place.

## About C-DAC Hydearabad

Centre for Development of Advanced Computing (C-DAC), a Scientific Society of Ministry of Communications & Information Technology, Government of India, is primarily an R&D institution involved in design, development and deployment of Advanced Electronics and Information Technology Solutions, including the celebrated PARAM series of Supercomputers. The C-DAC, Hyderabad is working in R&D with a focus on system level programming, web technologies and embedded programming in the application domains of Network Security, e-learning, Ubiquitous Computing, India Development Gateway (www.indg.in), Supply Chain Management and Wireless Sensor Networks.

## About ISEA

Looking at the growing importance for the Information Security, Department of Electronics & Information Technology has identified this as a critical area. Information Security Education and Awareness (ISEA) Project was formulated and launched for over a period of five years. One of the activities under this programme is to widely generate information security awareness to children, home users and non-IT professionals in a planned manner. C-DAC Hyderabad has been assigned the responsibility of executing this project by Department of Information Technology, Ministry of Communications and Information Technology, Government of India. As part of this activity, C-DAC, Hyderabad has to prepare the Information Security awareness material, coordinate with Participating Institutes (PIs) in organizing the various Information Security awareness events.

**VISION**

Generate Information Security Awareness among Indian citizens to enable them to participate safely in Information Society .

# AUDITING WINDOWS SERVER

## Table of Contents

1.Introduction.....

2.Checklist .....

1.BIOS Security is not enabled .....

2.Low free disk space .....

1.File system is not NTFS .....

2.Multiple operating systems are enabled .....

3.Windows Server Backup is not implemented .....

4.Page file setting is incorrectly configured .....

5.Time zone setting is incorrectly configured .....

6.System is not updated with the latest Service Pack .....

7.Screen saver password is not enabled.....

8.Antivirus software is not installed .....

9.Antivirus signature is not updated .....

10.Weak SNMP settings.....

11.Administrator account is not renamed.....

12.Guest account is not disabled .....

13.Non-essential network protocols are enabled .....

14.Insecure setting of Terminal Services .....

15.Insecure setting of Internet CommuCDACations .....

16.Run list is not disabled .....

17.Insecurely configured Remote System Access.....

18.Non-essential services are enabled .....

19.Weak account policy.....

20.Non essential accounts are not disabled.....

21.Auditing and Logging is not enabled.....

22.Weak user rights .....

23.Incorrect configuration of security options .....

**24.Inadequate space allocation for Event viewer .....**

**25.Shares with insecure permission .....**

**26.Weak permissions on critical system files .....**

**27.Auto play is enabled .....**

**28.Remote Registry Access is enabled .....**

**29.Critical Security patches are not installed .....**

**30.Incorrect setting of Recycle bin.....**

**31.Incorrect setting of NTP server .....**

**Appendix 1 : Hardening Guidelines for IIS 7.0 .....**

**Appendix 2 : Change Tracking Sheet .....**

**Service Tracking Sheet.....**

**Account Policies .....**

**Audit Policy .....**

**User Rights Tracking Sheet .....**

**Security Options Tracking Sheet.....**

**Permission on shared objects.....**

**Permission on critical system files .....**

**Appendix 2: References.....**

# 1. Introduction

This document is a security hardening guide for the Microsoft Windows Server 2008 R2 operating system. This guide was tested against Microsoft Windows Server 2008 R2. It summarizes a checklist of the configuration settings that constitute a secure server to safeguard against potential hackers and crackers. It provides contextual descriptions of each checklist item along with details of what the setting means, it's possible values followed by recommended mitigating strategies. The recommendations are intended to provide helpful information to administrators attempting to evaluate or improve the security of their systems. Proper use of the Recommendations requires careful analysis and adaptation to specific user requirements. The Recommendations are not in any way intended to be a "quick fix" solutions for securing server's operating system. For server specific recommendations a Vulnerability Assessment on the server is required.

Since IIS 7.0 is the default web server shipped out with the operating system, it is advisable to harden the web server along with the operating system. A few critical security guidelines are provided in Appendix 1.

The administrator should use the Change Tracking Sheet in Appendix 2 to note all the current settings before making changes as per this guide. The administrator should test all the recommended settings in this guide before implementing in the production environment.

**Recognition**

The following resources were referred during the development of this guide.

1. Security Configuration Benchmark for Microsoft Windows Server 2008, released by The Centre for Internet Security (CIS)

2. Microsoft's Security Compliance Management Toolkit

# 1. Checklist

The critical security settings are detailed hereafter. It is recommended to test these settings in a testing environment before making changes in the production environment.

| Title | 1. BIOS Security is not enabled |
|---|---|
| ***Description*** | In the BIOS setup, a password can be configured so that each time the system is booted it asks the user for the password. |
| ***Risk Rating*** | High |

**Impact**: A malicious user with physical access to the machine can boot from a rescue floppy or a CD-ROM and gain root access. Once that is done, it is easy for him to mount and modify various file systems, add new administrators and misuse the system.

**Solution**: In order to prevent malicious users from gaining root access, the following changes need to be made in the BIOS:

1. Set Supervisor Password.
2. After the installation, disable booting from the Floppy or the CD-ROM drive.

**Note:** In a secured place like CDAC Data Centre, where physical access to the servers is restricted, setting up of the BIOS password is at the discretion of the Administrator.

| Title | 2. Low free disk space |
|---|---|
| ***Description*** | Free disk space is an important parameter that can affect the performance, security and availability of the system. |
| ***Risk Rating*** | Medium |

**Impact**: System can become slow and programs can also fail. This might lead to denial of service condition.

**Solution:** Ensure at least 1 GB space is free on the logical drives. Ensure additional free space if you have temporary directories on the same drive.

**NOTE:**

✓ It is recommended to maintain multiple logical partition drives instead of just one drive (disk space should be distributed across partitions).

✓ Maintaining more free space in the system partition drive than other logical partition drives is functionality wise more desirable.

✓ It is advisable to segregate data & application files from system files and should be kept in logical partition drives & NOT on the system partition drive.

✓ In case of a new System installation of any Server in IDC the minimum space allocation for initial OS configuration for system partition drive should be relatively more for better System performance.

| Title | 1. File system is not NTFS |
|---|---|
| *Description* | NTFS is a secure file system that enables administrators to configure security features including discretionary access control. |
| *Risk Rating* | Medium |

**Impact:** Granular user permissions cannot be configured in file systems other than NTFS. This can lead to unauthorized access to critical information.

**Solution:** Make sure that all partitions on server are formatted using NTFS. If necessary, use the convert utility to non-destructively convert FAT partitions to NTFS. To convert a FAT/FAT32 partition into NTFS type partition, use the following command:

```
convert x: /fs:ntfs (where x is the drive letter)
```

| Title | 2. Multiple operating systems are enabled |
|---|---|
| *Description* | Multiple operating systems might be installed on the same server. |
| *Risk Rating* | Medium |

**Impact:** Multiple operating systems provide alternate methods to unauthorized users to access critical system information.

**Solution:** Make sure that only one operating system is installed. Remove the operating systems not needed for the normal functioning of the server and format the drives on which they are installed.

| Title | 3. Windows Server Backup is not implemented |
|---|---|
| ***Description*** | The windows backup (Ntbackup.exe) feature available in Windows Server 2003 is replaced by 'Windows Server Backup' (Wbadmin command), a new backup and recovery technology. Windows Server Backup uses the Volume Shadow Copy Service (VSS) and block-level backup technology to backup and recover the operating system, files & folders and volumes. It provides an option for the bare-metal recovery state. |
| ***Risk Rating*** | High |
| ***Reference*** | http://technet.microsoft.com/en-us/library/cc770266(v=ws.10).aspx |

**Impact:** Complete system recovery is not possible without Windows Server Backup; this can lead to system non-availability.

**Solution:** It is recommended to backup system state at regular intervals of time using Windows Server Backup.

To install the Windows Server Backup:

1. Navigate to 'Server Manager'. Click on the 'Features' in the left pane. Then click on 'Add Features' in the right page. This opens the Add Features Wizard.

2. In the 'Add Features' Wizard, on the 'Select Features' screen, expand 'Windows Server Backup Features' and then select the check boxes for Windows Server backup and Command-line Tools.

3. Click on the 'Next' button to proceed to the 'Confirmation' screen.

4. On the Confirm Installation Selections page, review the choices that you made, and then click Install. If there is an error during the installation, it will be noted on the Installation Results page.

5. Click Start, click Server Manager, in the left pane click Features, and then in the right pane click Add Features. This opens the Add Features Wizard.

6. Then, to access these backup and recovery tools, do the following:

    a. To access the Windows Server Backup snap-in, click Start, click Administrative Tools, and then click Windows Server Backup.

    b. To access and view the syntax for Wbadmin, click Start, right-click Command Prompt, and then click Run as administrator. At the prompt, type: wbadmin /?

    c. For instructions to access and view the Help for the Windows Server Backup cmdlets, see GettingStarted.rtf at: <*systemdrive*>:\Windows\System32\WindowsPowerShell\v1.0\Documents\<*language*>.

| Title | 4. Page file setting is incorrectly configured |
|---|---|
| ***Description*** | Virtual memory mechanism in Operating Systems requires disk space to be reserved for swapping operation. |
| ***Risk Rating*** | Medium |

**Impact:** System might become slow and system misbehavior can lead to non-availability of system.

**Solution:**

1. Set the page file to a minimum of RAM plus 300 MB or 1 GB, whichever is larger up to a maximum of 3 times the RAM or 4GB, whichever is larger.
2. Maximum and Initial size should be same.

| Title | 5. Time zone setting is incorrectly configured |
|---|---|
| ***Description*** | Time zone setting provides the reference in the enterprise for all activities that are logged in a system. |
| ***Risk Rating*** | Medium |

**Impact:** Correlation of logs and establishment of timeline for any malicious activity detected cannot be done.

**Solution:** Set time zone to "(GMT+5:30) Calcutta, Chennai, Mumbai, New Delhi"

| Title | 6. System is not updated with the latest Service Pack |
|---|---|
| ***Description*** | Service packs provide the OS enhancements and latest updates against vulnerabilities. |
| ***Risk Rating*** | High |

**Impact:** System can get affected by the latest vulnerabilities.

**Solution:**

1. Install latest the service pack (e.g. SP1).
2. Download the SP1 as follows:
    a. Browse to http://technet.microsoft.com.
    b. Navigate to the "Downloads" menu.
    c. Click on "Windows Server 2008 R2" under the "Operating Systems" category.

d. Select “Windows Servers” under product, “2008” under version and “Service Packs” under download type for Find Downloads section.

e. Click on “Download Windows Server 2008 R2 with Service Pack 1”. (The corresponding URL is http://technet.microsoft.com/en-us/evalcenter/ee175713.aspx).

| Title | **7. Screen saver password is not enabled** |
|---|---|
| ***Description*** | Windows allows server console to be locked after a particular period of inactivity and requires authentication for unlocking the console. |
| ***Risk Rating*** | Medium |

**Impact:** An intruder can use an unattended console for manipulating system settings for gaining unauthorized access.

**Solution:**

1. Enable screen saver password.

a. Click **Start** > **Run** and type **gpedit.msc**.

b. Expand **User Configuration > Administrative Template > Control Panel > Personalization** container.

c. Select **Password protect the screen saver** and **Enable** it.

2. Set the screen saver timeout to 5 minutes by setting the following registry

HKEY_CURRENT_USER\Control Panel\Desktop\ScreenSaveTimeOut=300

3. Set the screen saver grace period to zero.

HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\ScreenSaverGracePeriod=0 (this entry does not exist in the registry by default. It needs to be created as a REG_DWORD)

| Title | 8. Antivirus software is not installed |
|---|---|
| ***Description*** | Antivirus software protects systems from virus infection. Properly configured and updated antivirus software should be implemented on systems. |
| ***Risk Rating*** | High |

**Impact:** Virus infection can cause systems to malfunction leading to denial of service. Infected systems can also be used as intermediaries for infecting other systems.

**Solution:** Install antivirus software and configure regular updates of signature patterns.

**How to Check:** Click **Start** > **Settings** > **Control Panel**, open **Add/Remove programs** and check Antivirus software is installed or not.

| Title | 9. Antivirus signature is not updated |
|---|---|
| ***Description*** | Antivirus signature contains the signature patterns of viruses. Latest signatures protect systems from recent virus infection. |
| ***Risk Rating*** | High |

**Impact:** Servers will not be protected from new virus attacks.

**Solution:** Update the antivirus signatures.

**How to Check:** Open Trend Micro Console>Help>About>Check for the last Antivirus Update date.

| Title | 10.Weak SNMP settings |
|---|---|
| ***Description*** | SNMP is a protocol that is widely used for server monitoring and management. SNMP agent can be accessed using a password referred to as community string. Default SNMP security is based on a Community Name “Public” or “Private”. The Community Name acts like a password in the case of SNMP connectivity.<br><br>Note: This setting is ONLY applicable to servers where SNMP service is running. |
| ***Risk Rating*** | Medium |

**Impact:** Malicious user can use default community strings and modify system settings without authorization.

**Solution:**

1. Use complex community string.
   a. Go to **Start > Programs > Administrative Tools > Services**.
   b. Double click **SNMP service** and click on the **Security Tab**.
   c. Change the community names from PUBLIC or PRIVATE to a non-guessable string.
   d. Read only community permission should be given.

| Title | 11.Administrator account is not renamed |
|---|---|
| *Description* | A default administrator user name is created during installation. This should be renamed for high security levels. |
| *Risk Rating* | Medium |

**Impact:** Malicious user can try to compromise the system using administrator account.

**Solution:** Rename the Administrator account from computer management.

**How to Check:**

1. Click **Start** > **Run** and type **compmgmt.msc**.
2. Expand **Local User & Groups** > **Users** container.
3. Check the Administrator account is renamed or not.

| Title | 12.Guest account is not disabled |
|---|---|
| *Description* | A guest account is created by default during installation. This should be disabled for high security levels. |
| *Risk Rating* | Medium |

**Impact:** Malicious user can enter the system using guest account.

**Solution:** Disable the guest account from computer management.

**How to Check:**

1. Click **Start** > **Run** and type **compmgmt.msc**.
2. Expand **Local User & Groups** > **Users** container

3. Check the Guest account is disabled or not.

| Title | 13.Non-essential network protocols are enabled |
|---|---|
| ***Description*** | Multiple protocols are enabled during a default installation of Operating System. |
| ***Risk Rating*** | Medium |

**Impact:** New/Old vulnerabilities found in protocols can be used by malicious users for break in.

**Solution:**

1 Only TCP/IP protocol should be the protocol of choice unless otherwise driven by legacy application requirements.

2 NetBIOS over TCP/IP should be disabled.

3 For Web and DNS servers, disable:

a. Client for Microsoft Networks.

b. File and Print sharing services for Microsoft Networks.

4 TCP/UDP PORTS can be restricted by using windows firewall (In Microsoft Windows 2008, windows firewall is bound to a specific network profile instead of being bounded to specific Network Interface Card as in case of Windows XP. Thus connectivity to TCP/UDP ports can now be restricted using different firewalls rules that are applicable to all the network interface cards).

**How to Check:**

To check non-essential protocols:

1 Right click on My Network Places on the desktop, select Properties.

2 Right click on Local area connection, select Properties.

3 Check the installed services and protocols. The following services and protocols are installed by default in the server and they are required for server operation.

a. TCP/IP Protocol

b. Client of Microsoft Networks. (Should be disabled in Web & DNS Server)

c. File and Print sharing services for Microsoft Network. (Should be disabled in Web & DNS Server)

To check NetBIOS over TCP/IP status:

1 Right click on My Network Places on the desktop, select Properties.

2 Right click on Local area connection, select properties.

3 Double click on TCP/IP protocol, click on Advanced.

4 Go to WINS tab and check Disable NetBIOS over TCP/IP is selected or not.

| Title | **14. Insecure setting of Terminal Services** |
|---|---|
| ***Description*** | Terminal services will enable the user to access Windows based programs that are installed on the terminal server remotely. The settings to such services are insecurely configured with the default installation of the Operating System. |
| ***Risk Rating*** | Medium |

**Impact:** Terminal services can be accessed by the unauthorized users, if they are configured insecurely.

**Solution:**

1. Click **Start > Run** and type **gpedit.msc**.

2. Expand **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host** container.

3. Check the effective settings and compare with the following table:

| # | *Setting Name* | *Description* | *Default Setting* | *Suggested Setting* |
|---|---|---|---|---|
| 1. | Always prompt client for password upon connection | Users have an option to store both their username and password when they create a new Remote Desktop connection shortcut. This setting defines whether terminal services will prompt for a password even if it was already provided in the Remote Desktop Connection client.<br><br>If the status is set to enabled, users cannot automatically log on to Remote Desktop Services, even if they already provided the password in the Remote Desktop Connection client.<br><br>If the status is set to Not Configured, automatic logon is not configured at the Group Policy Level. However, an administrator can still enforce password prompting by using the Remote Desktop Host Configuration tool.<br><br>If the status is disabled, then the attacker who have physical access to the user computer can connect to the Terminal Server through Remote Desktop | ✓ Not Configured | ✓ Enabled |

| # | Setting Name | Description | Default Setting | Suggested Setting |
|---|---|---|---|---|
| | | Connection client, even though he does not know the password. | | |
| 1. | Set client connection encryption level | This setting specifies whether to require the use of a specific encryption level to secure commuCDACations between clients and Remote Desktop (RD) Session Host servers during Remote Desktop Protocol connections.<br>The following encryption methods are available.<br>• High<br>• Client Compatible<br>• Low<br>Note: 128-bit encryption for terminal services will help ensure the confidentiality and integrity of data sent and received. | ✓ Not Configured | ✓ Enabled: High Level |
| 1. | Do not allow drive redirection | This setting specifies whether to prevent the mapping of client drives in a Remote Desktop Services session (drive redirection).<br>By default, an RD Session Host server maps client drives automatically upon connection. Mapped drives appear in the session folder tree in Windows Explorer. This setting can be used to override this behaviour.<br>If the status is set to Enabled, client drive redirection is not allowed in Remote Desktop Services sessions.<br>If the status is set to Not Configured, client drive redirection is not configured at the Group Policy Level. However, an administrator can still disable client drive redirection by using the Remote Desktop Host Configuration tool.<br>Redirecting a local drive to a remote Terminal Services session may expose local drives contents to threats against its confidentiality, integrity and availability. | ✓ Not Configured | ✓ Not configured |
| 1. | Do not allow password to be saved. | This setting defines whether passwords can be saved on the user's computer for accessing the terminal services.<br>If the setting is enabled, the password saving | ✓ Not Configured | ✓ Disabled |

| # | Setting Name | Description | Default Setting | Suggested Setting |
|---|---|---|---|---|
| | | checkbox in Remote Desktop Connection clients will be disabled and users will no longer be able to save password.<br><br>If the setting is disabled or not configured, the user will be able to save passwords using the Remote Desktop Connection clients.<br><br>If the user account that has saved passwords is compromised, an attacker can leverage saved passwords to access other servers. | | |

| Title | 15. Insecure setting of Internet CommuCDACations |
|---|---|
| Description | Internet can be used by the users to print over HTTP and publish their files and folders over Web. Such settings are insecurely configured with the default installation of the Operating System. |
| Risk Rating | Medium |

**Impact:** Insecure configuration of Internet CommuCDACations may impact the confidentiality, integrity and availability of the user data.

**Solution:**

1. Click **Start > Run** and type **gpedit.msc**.

2. Expand **Computer Configuration > Administrative Templates > System > Internet CommuCDACation Management > Internet CommuCDACation Settings** container.

3. Check the effective settings and compare with the following table:

| # | Setting Name | Description | Default Setting | Suggested Setting |
|---|---|---|---|---|
| 1. | Turn off downloading of print drivers over HTTP | This setting defines whether to allow the users to download print driver packages over HTTP. To set up HTTP printing, non-inbox drivers need to be downloaded over HTTP.<br><br>If the setting is enabled, print drivers will not be | ✓ Not Configured | ✓ Enabled |

| # | Setting Name | Description | Default Setting | Suggested Setting |
|---|---|---|---|---|
| | | downloaded over HTTP.<br><br>If the setting is disabled or not configured, the user will be able to download print drivers over HTTP.<br><br>Preventing users from downloading print drivers over HTTP may reduce the probability of introducing drivers that impact the system's stability and security.<br><br>Note: This setting does not prevent the client from printing to printers on the Intranet or the Internet over HTTP. It only prohibits downloading drivers that are not already installed locally. | | |
| 1. | Turn off the "Publish to Web" task for files and folders | This setting defines whether the tasks "Publish this file to the Web", "Publish this folder to the Web", and "Publish the selected items to the Web", are available from File and Folder Tasks in Windows folders. The Web Publishing Wizard is used to download a list of providers and allow users to publish content to the Web.<br><br>If the setting is enabled, these tasks are removed from the File and Folder tasks in Windows folders.<br><br>If the setting is disabled or not configured, the tasks will be shown.<br><br>Enabling this setting will reduce the probability of user publishing confidential or sensitive information to a public service. | ✓ Not Configured | ✓ Enabled |
| 1. | Turnoff Internet download for Web publishing and online ordering wizards | This setting defines whether Windows should download a list of providers for the Web publishing and online ordering wizards. These wizards allow users to select from a list of companies that provide services such as online storage and photographic printing.<br><br>If the setting is enabled, Windows will not download providers and only the service providers that are cached in the local registry will be displayed.<br><br>If the setting is disabled or not configured, a list of providers will be downloaded when the user uses the Web publishing or online ordering wizards.<br><br>Enabling this setting will reduce possibility of a user | ✓ Not Configured | ✓ Enabled |

| # | Setting Name | Description | Default Setting | Suggested Setting |
|---|---|---|---|---|
| | | unknowingly downloading malicious content. | | |
| 1. | Turn off printing over HTTP | This setting defines whether to allow printing over HTTP from client. Printing over HTTP allows a client to print to printer on the intranet as well as the Internet.<br><br>If the setting is enabled, it prevents the clients from printing to Internet printers over HTTP.<br><br>If the setting is disabled or not configured, user will be able to choose to print to Internet printers over HTTP.<br><br>HTTP is a clear text protocol. Disabling this setting, may impact the confidentiality and integrity of the print data. | ✓ Not Configured | ✓ Enabled |
| 1. | Turn off Search Companion content file updates | This setting defines whether Search Companion should automatically download content updated during local and Internet searches. When the user searched the local machine or the Internet, Search Companion occasionally connects to Microsoft to download an updated privacy policy and additional content files used to format and display results.<br><br>If the setting is enabled, Search Companion will not download content updates during searches.<br><br>If the setting is disabled or not configured, Search Companion will download content updates during searches.<br><br>Enabling this control reduces the probability of a user unknowingly revealing sensitive information via the topics they are searching for. | ✓ Not Configured | ✓ Enabled |
| 1. | Turn off the Windows Messenger Customer Experience Improvement Program | This setting defines whether Windows Messenger collects anonymous information about how Windows Messenger software and service is used. With the Customer Experience program, users can allow Microsoft to collect anonymous information about how the product is used. This information is used to improve the product in future releases.<br><br>If the setting is enabled, Windows Messenger will not collect usage information. | ✓ Not Configured | ✓ Enabled |

| # | Setting Name | Description | Default Setting | Suggested Setting |
|---|---|---|---|---|
| | | If the setting is disabled, Windows Messenger will not collect usage information.<br><br>If the setting is not configured, users have the choice to opt-in and allow information to be collected.<br><br>Enabling this setting will eliminate any risk of information disclosure. | | |
| 1. | Turn off Windows Update device driver searching | This setting defines whether Windows searches Windows Update for device drivers when no local drivers for a device are present.<br><br>If the setting is enabled, Windows Update will not be searched when a new device is installed.<br><br>If the setting is disabled, Windows Update will always be searched when a new device is installed.<br><br>If the setting is not configured, searching Windows Update will be optional when installing a device.<br><br>Enabling this setting prevents users from downloading and installing device drivers that reduce system stability and security. | ✓ Not Configured | ✓ Not Defined |

| Title | **16.Run list is not disabled** |
|---|---|
| ***Description*** | Run list is the list of programs that Windows run automatically when it starts. Run once list is the list of programs that Windows run automatically the next time it starts. The settings to process the lists are not disabled. |
| ***Risk Rating*** | Medium |

**Impact:** Malicious user can execute arbitrary code upon reboot.

**Solution:**

1. Click **Start > Run** and type **gpedit.msc**.
2. Expand **Computer Configuration > Administrative Templates > System > Logon** container.
3. Check the effective settings and compare with the following table:

| # | *Setting Name* | *Description* | *Default Setting* | *Suggested Setting* |
|---|---|---|---|---|
| **1.** | Do not process the legacy run list. | This setting defines whether the system has to ignore the customized run list. The user can create a customized list of additional programs and documents that the Windows run automatically when it starts. These programs are added to the standard run list of programs and services that the system starts.<br>If the setting is enabled, the system ignores the run list.<br>If the setting is disabled or not configured, the system adds any customized run list configured to its run list. | ✓ Not Configured | ✓ Not Configured |
| **1.** | Do not process the run once list. | This setting defines whether the system has to ignore the customized run once list. The user can create a customized list of additional programs and documents that the Windows run automatically when the system starts next time(but not thereafter). These programs are added to the standard run list of programs and services that the system starts.<br>If the setting is enabled, the system ignores the run once list.<br>If the setting is disabled or not configured, the | ✓ Not Configured | ✓ Not Configured |

| # | Setting Name | Description | Default Setting | Suggested Setting |
|---|---|---|---|---|
| | | system adds any customized run once list configured to its run list. | | |

| Title | 17. Insecurely configured Remote System Access |
|---|---|
| Description | Remote system access will provide the remote party to control the local system. Such services are not securely configured in the default installation of the operating system. |
| Risk Rating | Medium |

**Impact:** The security status of the remote system may be affected.

**Solution:**

1. Click **Start > Run** and type **gpedit.msc**.
2. Expand **Computer Configuration > Administrative Templates > System > Remote Assistance** container.
3. Check the effective settings and compare with the following table:

| # | Setting Name | Description | Default Setting | Suggested Setting |
|---|---|---|---|---|
| **1.** | Offer Remote Assistance | This setting defines whether Windows will allow unsolicited offers to provide remote assistance to the local user. Remote assistance provides the remote party with the ability to view or control the local system.<br>If the setting is enabled, the users of the system can get assistance from their support staff using Remote Assistance.<br>If the setting is disabled or not configured, the users of the system cannot get assistance from their support staff using Remote Assistance. | ✓ Not Configured | ✓ Not Defined |
| **1.** | Solicited Remote Assistance | This setting defines whether Windows will allow solicited offers to provide remote assistance to the local user. Remote assistance provides the remote party with the ability to view or control the local | ✓ Not Configured | ✓ Not Defined |

| # | Setting Name | Description | Default Setting | Suggested Setting |
|---|---|---|---|---|
| | | system.<br><br>If the setting is enabled, the users of the system can use e-mail or file transfer to ask someone for help. Also, users can use instant messaging programs to allow connections to the computer.<br><br>If the setting is disabled, cannot use e-mail or file transfer to ask someone for help. Also, users cannot use instant messaging programs to allow connections to the computer.<br><br>If the setting is not configured, users can enable or disable Solicited Remote Assistance themselves in System Properties in Control Panel. | | |
| The path to configure the below setting is<br>1. Click **Start > Run** and type **gpedit.msc**.<br>2. Expand **Computer Configuration > Administrative Templates > Windows Components > NetMeeting** container. | | | | |
| **1.** | Disable remote desktop sharing | This setting defines whether a user is allowed to share their desktop using NetMeeting.<br><br>Enabling this setting will reduce the remote attack surface of the system. | ✓ Not Configured | ✓ Enabled |

| Title | 18.Non-essential services are enabled |
|---|---|
| ***Description*** | Multiple services are enabled during a default installation of Operating System. |
| ***Risk Rating*** | High |

**Impact:** New/Old vulnerabilities found in unused applications/services can be used by malicious users for break- in.

## Solution:

1. Disable the services that are not required for the server.
   a. Go to Start>Programs>Administrative Tools>Services.
   b. Select the services listed below.
   c. Right click on the service and choose disabled.
   d. Restart the computer after disabling all services.
2. A minimal list of services that can be disabled is given below.
3. The administrator should review each of the services before disabling them so as not to affect the current operating environment of the server. The services that are required should not be disabled.

## Note:

1. Before changing the service settings the administrator should take the settings backup as follows:
   - ✓ Go to **Start > Programs > Administrative Tools > Services**.
   - ✓ Right click on the "**Services**" entity on the left panel.
1. Use the Change Tracking Sheet in Appendix 1 to track all the changes.

| # | Full Service Name | Description | Depends On | Depended By | Implication | Exception |
|---|---|---|---|---|---|---|
| | Alerter | Notifies selected users and computers of administrative alerts | ✓ Work-station | | Programs that use administrative alerts will not receive them. | |
| | ClipBook | Enables the Clipbook viewer to create and share pages of data to be viewed by remote computers | ✓ Network DDE<br>✓ Network DDE DSDM | | Clipbrd.exe will time out on startup and notify the user that it cannot be started and remote access is not available. However, Clipbrd.exe can still be used to view the local Clipboard (where data | |

| # | Full Service Name | Description | Depends On | Depended By | Implication | Exception |
|---|---|---|---|---|---|---|
| | | | | | is stored when a user highlights text and then goes to the Edit menu and selects Copy, or types Ctrl+C) | |
| | Cluster Service | Controls all aspect of the server cluster operation and manages the cluster database | ✓ Remote Procedure Call<br>✓ Windows Time | | Clustering is unavailable | Enable if server acts as Server Clusters/Network Load Balancing Clusters |
| | DHCP Client | Manages the network configuration by registering and updating IP addresses and Domain Name Server names | | | The system will be unable to obtain an IP address, WINS information, etc from a DHCP server & will need to be configured with a static IP address | Enable if the server uses DHCP to get its IP address from a DHCP Server |
| | DHCP Server | The service automatically allocates IP addresses & advanced network setting configurations (like DNS servers, WINS servers etc) to all DHCP clients | ✓ Remote Procedure Call (RPC)<br>✓ Security Accounts Manager | | Clients will be unable to get the addressing information, which could result in a loss of network connectivity (if DHCP is being used) | Enable if the server acts as a DHCP Server |
| | Distributed File System | It integrates different file shares into a single logical namespace enabling the users to access the network data through the logical namespace | ✓ Server<br>✓ Work-station | | Users will be unable to access distributed files using the logical namespace and will instead need to specifically target an individual server to get the required information | Enable if the server is a Domain Controller |
| | Distributed Link Tracking | It enables the Distributed Link | ✓ Remote Procedure | | | Enable if the server is a Domain |

| # | Full Service Name | Description | Depends On | Depended By | Implication | Exception |
|---|---|---|---|---|---|---|
| | Server | Tracking Client service to track linked documents that have been moved to a location in another NTFS volume in the same domain | Call (RPC) | | | Controller |
| | DNS Server | It enables DNS name resolution by answering queries and update requests for Domain Name Server(DNS) names | ✓ NT LM Security Support Pro-vider<br>✓ Remote Procedure Call (RPC) | | Access to resources cannot be made by name. Instead resources can be accessed by IP addresses. There could be serious implications for Active Directory lookups | Enable if the server is a DNS Server |
| | Fax Service | It enables to send & receive faxes | ✓ Plug and Play<br>✓ Print Spooler<br>✓ Remote Procedure Call (RPC)<br>✓ Telepho-ny | | | Enable if the server is being used as a fax server |
| | File Replication | Maintains file synchronization of file directory contents among multiple servers. | ✓ Event Log<br>✓ Remote Procedure Call (RPC) | | File replication will not take place resulting in an impaired Domain Controller | Enable if the server is a Domain Controller |
| | File Server for Macintosh | It enables Macintosh users to store and access files on Windows server machines | ✓ Work-station | | Apple Mac users cannot access files from a Microsoft Windows server | |
| | FTP Publishing Service | It provides File Transfer Protocol(FTP) | ✓ IIS Ad-min Service | | | Enable if files are either uploaded or |

| # | Full Service Name | Description | Depends On | Depended By | Implication | Exception |
|---|---|---|---|---|---|---|
| | | connectivity and administration through the Internet Information Services(IIS) snap-in. | | | | downloaded from the server using FTP.<br>It is recommended to use Secure FTP instead of FTP. |
| | IIS Admin Services | It allows administration of Internet Information Services (IIS). | ✓ Protect-ed Storage<br>✓ Remote Procedure Call (RPC) | ✓ FTP Publishing Service<br>✓ Net-work News Transport Protocol (NNTP)<br>✓ Simple Mail Transport Protocol (SMTP)<br>✓ World Wide Web Publishing Service | Web, FTP, NNTP & SMTP services will not run on the server<br>Stopping this service will automatically stop the following services:<br>✓ FTP Publishing Service<br>✓ SMTP<br>✓ NNTP<br>✓ WWW Publish-ing Service | Enable if the server is a Web Server |
| | Indexing Service | It indexes all textual information in files and documents. | ✓ Remote Procedure Call (RPC) | | Searching is done by traversing the folder hierarchy and scanning each file for the requested string leading to slower response time | |
| | Internet Connection Sharing | Provides network address translation, addressing, and name resolution services for a small home or small office network. | ✓ Remote Access Con-nection Manager | | Network services such as Internet sharing, name resolution, addressing will be unavailable | Enable if the servers is an Internet Gateway |
| | Messenger | It transmits net send & Alert service messages between clients and servers. | ✓ Remote Procedure Call (RPC)<br>✓ Work- | | Alert messages will not be transmitted | |

| # | Full Service Name | Description | Depends On | Depended By | Implication | Exception |
|---|---|---|---|---|---|---|
| | | This service is not related to Windows Messenger. | station | | | |
| | NetMeeting Remote Desktop Sharing | Allows authorized people to remotely access your Windows desktop using NetMeeting. | | | The NetMeeting display driver is unloaded and remote desktop sharing is unavailable | |
| | Network DDE | It provides network transport and security for dynamic data exchange (DDE) for programs running on the same computer or on different computers. | ✓ Network DDE DSDM | ✓ Clip-Book | DDE transport and security will be unavailable | |
| | Network DDE DSDM | Manages shared dynamic data exchange and is used by Network DDE | | ✓ Net-work DDE | DDE network shares will be unavailable | |
| | Network News Transfer Protocol(NNTP) | It facilitates to distribute network news messages to NNTP servers and clients (newsreader) on the internet. NNTP is designed so that news articles are stored on a server in a central database, thus enabling a user to select specific items to read. | ✓ IIS Ad-min Service | | Client computers cannot connect, read or posts news to NNTP server. | Enable the service if it is required to use a news client such as Microsoft Outlook Express to retrieve newsgroups from the NNTP server to read headers & bodies of the articles in each newsgroup. |
| | Print Server for Macintosh | It enables Macintosh clients to route printing to a print | ✓ Print Spooler | | Printing will be unavailable to | |

| # | Full Service Name | Description | Depends On | Depended By | Implication | Exception |
|---|---|---|---|---|---|---|
| | | spooler located on a computer running Windows 2008 Server. | | | Macintosh clients | |
| | Print Spooler | It manages all local & network print queues and controls all printing jobs. | ✓ Remote Procedure Call (RPC) | ✓ Fax Service | Printing on the local machine will be unavailable | Enable if printing/faxing is required from the server |
| | Remote Access Auto Connection Manager | It creates a connection to a remote network whenever a program references a remote DNS or NetBIOS name or address. It detects unsuccessful attempts to connect to a remote network or computer and automatically dial the connection that was last used to reach this remote device. | ✓ Remote Access Connection Manager<br>✓ Telephony | | Users will need to manually set up connections to remote computers | |
| | Remote Registry | Allows remote registry manipulation. | ✓ Remote Procedure Call (RPC) | | The registry on the local computer can only be modified locally | Enable if registry is to be remotely maintained by the administrator |
| | Remote Storage Server | It stores infrequently used files in a secondary storage media. Further this service allows the Remote Storage application to notify the user when an offline file had been accessed. | ✓ Event Log<br>✓ Remote Procedure Call (RPC)<br>✓ Removable Storage<br>✓ Task Scheduler | | Files cannot be moved to or retrieved from the secondary storage media | Enable if remote storage (like tape) is being used |

| # | Full Service Name | Description | Depends On | Depended By | Implication | Exception |
|---|---|---|---|---|---|---|
| | Removable Storage | It manages, catalogs removable media & operates automated removable media devices. | ✓ Remote Procedure Call (RPC) | ✓ Remote Storage Server | | Enable if remote storage (like tape) is being used |
| | Routing and Remote Access | It provides multiprotocol LAN-to-LAN, LAN-to-WAN, VPN, and network address translation (NAT) routing services. In addition, Routing and Remote Access also provides dial-up and VPN remote access services. | ✓ NetBIOSGroup<br>✓ Remote Procedure Call (RPC) | | If this service is stopped or disabled, the remote access server cannot accept incoming RAS, VPN, or demand-dial connections, and routing protocols are not received or transmitted. | Enable if remote access, VPN connections, dial-on-demand connections and routing protocols are required |
| | Simple Mail Transport Protocol (SMTP) | It transport the electroCDAC mail across the network | ✓ IIS Admin Service | | Mail will not be transported across the network. | Enable if e-mail replication and forwarding are required |
| | Smart Card | It manages and controls access to a smart card inserted into a smart card reader attached to the computer | ✓ Plug and Play | ✓ Datakey's Token Service | This computer will be unable to read smart cards. | Enable if the server is required to read smart cards |
| | SNMP Service | It allows incoming SNMP requests to be serviced by the local computer | ✓ Event Log | | The computer will not respond to SNMP requests. If the computer is being monitored by network management tools, those tools cannot collect data from the computer nor control | Enable if the server is being monitored by network management tools through the SNMP service |

| # | Full Service Name | Description | Depends On | Depended By | Implication | Exception |
|---|---|---|---|---|---|---|
| | | | | | its functionality through the SNMP service. | |
| | SNMP Trap Service | It receives trap messages generated by remote or local SNMP agents and forwards the messages to SNMP management programs running on this computer | ✓ Event Log | | SNMP based programs on this computer cannot receive SNMP trap messages | Enable if the server is being monitored by network management tools through the SNMP service |
| | Telnet | It allows a remote user to log on to the system and run console programs by using various TCP/IP Telnet clients, including UNIX & WINDOWS based computers | ✓ Remote Procedure Call (RPC) | | Remote users will not be able to connect to the computer using telnet clients | Enable if telnet is being used. It is recommended to use Secure Shell instead of telnet |
| | Terminal Services[1] | It allows multiple users to connect interactively to a terminal server & allows users to access | | | Remote users cannot use Remote Desktop | Enable if remote administrator is required |

[1] If Terminal Service is enabled then Encrypted RDP-Tcp connection should be used.

- ✓ Go to **Start > Programs > Administrative Tools > Terminal Services Configuration**.
- ✓ Right click on the "**RDP-Tcp**" connection & select "**properties**".
- ✓ In the "**General Tab**" Choose the encryption level "**Client Compatible**" (All data sent between the client and the server is protected by encryption based on the maximum key strength supported by the client).
- ✓ If supported, higher encryption levels (**High**/**FIPS Compliant**) can be enabled**.**

| # | Full Service Name | Description | Depends On | Depended By | Implication | Exception |
|---|---|---|---|---|---|---|
| | | desktops and applications on remote computers leading to access another user's desktop for administrative purposes. | | | | |
| | World Wide Web Publishing Service | It provides HTTP service for applications on the Windows platform | ✓ IIS Admin Service | | Web server will be unavailable | Enable if the server is a web server |

| Title | 19.Weak account policy |
|---|---|
| ***Description*** | Account policy helps administrators enforce strong user account policy. The account policy is required to control the user password characteristics, account lockout rules and Kerberos usage controls. |
| ***Risk Rating*** | High |

**Impact:** Users may use weak passwords or may not change passwords on a periodic basis; such user accounts can be compromised and can lead to unauthorized access. Also, the user accounts may be targeted for brute force attacks if the accounts are not locked are certain number of invalid login attempts.

**Solution:** Enforce account policy settings as shown below:

| # | Policy | Description | Suggested Setting |
|---|---|---|---|
| **Password Policy**<br>1. Click **Start > Run** and type **gpedit.msc**.<br>2. Expand **Computer Configuration > Windows Settings > Security Settings > Password Policy** container. | | | |
| 1. | Enforce Password History | Defines the number of unique passwords a user must leverage before a previously used password can be reused. | Minimum 24 Passwords (The default value is 24 passwords) |
| 2. | Maximum Password Age | Defines how many days a user can use the same password before it expires. | 90 Days |
| 3. | Minimum Password Age | Defines how many days a user must use the same password before it can be changed. | 1 Day |
| 4. | Minimum Password Length | Defines the minimum number of characters a user password must contain. | 8 Characters |
| 5. | Passwords Must Meet Complexity Requirements | Determines if new passwords are required to satisfy a certain level of complexity. | Enabled |
| 6. | Store Password Using Reversible Encryption | Defines whether the Windows can store the password using reversible encryption. | Disabled |
| **Account Lockout Policy**<br>1. Click **Start > Run** and type **gpedit.msc.** | | | |

| | | | |
|---|---|---|---|
| 2. Expand **Computer Configuration > Windows Settings > Security Settings > Account Lockout Policy** container. | | | |
| 1. | Account Lockout Duration | Defines the minimum number of minutes a user must wait before a locked account is unlocked. | 15 Minutes |
| 2. | Account Lockout Threshold | Defines the number of failed logon attempts before a user is locked out of an account. | 15 invalid logon attempts |
| 3. | Reset Account Lockout Threshold After | Following an unsuccessful logon, the system increments the count of invalid attempts for the account. This counter continues to increment until the lockout threshold is reached or the counter is reset. This setting defines how often the counter should reset. | 15 Minutes |
| **Kerberos Policy**<br>1. Click **Start > Run** and type **gpedit.msc**.<br>2. Expand **Computer Configuration > Windows Settings > Security Settings > Account Lockout Policy** container. | | | |
| 1. | Enforce user logon restrictions | Defines Kerberos-related attributes of domain user accounts, such as the Maximum lifetime for user ticket and enforce user logon restriction settings. | ✓ **Enterprise Member Server:** Not Defined<br>✓ **Enterprise Domain Controller:** Enabled |
| 1. | Maximum tolerance for computer clock synchronization | Defines maximum tolerance for computer related synchronization. | ✓ **Enterprise Member Server:** Not Defined<br>✓ **Enterprise Domain Controller:** 5 |
| 1. | Maximum lifetime for service ticket | Defines the maximum number of minutes that a granted session ticket can be used to access a service. | ✓ **Enterprise Member Server:** Not Defined<br>✓ **Enterprise Domain Controller:** 600 |
| 1. | Maximum lifetime for user ticket renewal | Defines the number of days during which a user's ticket-granting ticket (TGT) can be renewed. | ✓ **Enterprise Member Server:** Not Defined<br>✓ **Enterprise Domain Controller:** 7 days |
| 1. | Maximum lifetime for user ticket | Defines the maximum number of hours a user's ticket-granting ticket (TGT) may be used. | ✓ **Enterprise Member Server:** Not Defined |

| | | | |
|---|---|---|---|
| | | | ✓ **Enterprise Domain Controller:** 10 |

| | |
|---|---|
| **Title** | **20.Non essential accounts are not disabled** |
| ***Description*** | Accounts that are not essential for system or application requirements should be disabled. |
| ***Risk Rating*** | High |

**Impact**: Non-essential user accounts increase the likelihood of compromise by providing more accounts that can be used to gain unauthorized access.

**Solution**: Disable all accounts that do not meet system or application objectives.

| | |
|---|---|
| **Title** | **21.Auditing and Logging is not enabled** |
| ***Description*** | Audit enables administrators to monitor critical events in a Windows 2008 Server. |
| ***Risk Rating*** | High |

**Impact:** Malicious activities will not be detected. Early warning towards attempts at malicious access will go undetected.

**Solution:**

It is recommended to disable the following audit policy settings and use detailed audit policy settings.

- ✓ Audit Account Logon Events
- ✓ Audit Account Management
- ✓ Audit Directory service access
- ✓ Audit Logon Events
- ✓ Audit Object Access
- ✓ Audit Policy Change
- ✓ Audit Privilege Use
- ✓ Audit Process Tracking
- ✓ Audit System Events

Enforce detailed audit policy settings as shown below:

| # | Setting Name | Description | Suggested Setting |
|---|---|---|---|
| The path to configure the following settings is as below.<br>1. Click **Start > Run** and type **gpedit.msc**.<br>2. Expand **Computer Configuration > Windows Settings > Security Settings > Local Policies > Audit Policy** container.<br>3. Check the effective settings for Audit policy and compare with the following settings. | | | |
| 1. | Audit: Shut down system immediately if unable to log security audits | If this policy is enabled, it causes the system to halt if a security audit cannot be logged for any reason. Typically, an event will fail to be logged when the security audit log is full and the retention method specified for the security log is either Do Not Overwrite Events or Overwrite Events by Days.<br>If the security log is full and an existing entry cannot be overwritten and this security option is enabled, the following blue screen error will occur:<br>STOP: C0000244 {Audit Failed}<br>An attempt to generate a security audit failed.<br>To recover, an administrator must log on, archive the log (if desired), clear the log, and reset this option as desired. | ✓ Disabled<br>Note:<br>This option should be enabled for high business critical servers where security logs are a must. |
| 1. | Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit. | This setting causes Windows to respect audit subcategories in favor of the legacy audit policies. | Enabled |
| The path to configure the following settings is as below.<br>1. Click **Start > Run** and type **gpedit.msc**.<br>2. Expand **Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration > System Audit Policy – Local Group Policy Object> System** container.<br>3. Check the effective settings for Audit policy and compare with the following settings. | | | |
| 1. | Audit Policy: System: IPSec Driver | Defines whether Internet Protocol security (IPSec) driver activity is audited. | Success and Failure |
| 2. | Audit Policy: | Defines whether the audit is activated for changes in | Success and Failure |

| # | Setting Name | Description | Suggested Setting |
|---|---|---|---|
| | System: Security State Change | the security state of the system. | |
| 3. | Audit Policy: System: Security State Extension | Defines whether the audit is activated for the loading of extension code such as authentication packages by the security subsystem. | Success and Failure |
| 4. | Audit Policy: System: System Integrity | Defines whether the audit is activated for violations of integrity of the security subsystem. | Success and Failure |
| The path to configure the following settings is as below.<br>1. Click **Start > Run** and type **gpedit.msc**.<br>2. Expand **Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration > System Audit Policy – Local Group Policy Object> Logon/Logoff** container.<br>3. Check the effective settings for Audit policy and compare with the following settings. | | | |
| 1. | Audit Policy: Logon-Logoff: Logoff | Defines whether the audit is activated for when a user logs off from the system. | Success |
| 2. | Audit Policy: Logon-Logoff: Logon | Defines whether the audit is activated for when a user attempts to log on to the system. | Success<br>Note: For critical system servers, enable both 'Success and Failure'. |
| 3. | Audit Policy: Logon-Logoff: Special Logon | Defines whether the audit is activated when a special logon is used. | Success |
| The path to configure the following settings is as below.<br>1. Click **Start > Run** and type **gpedit.msc**.<br>2. Expand **Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration > System Audit Policy – Local Group Policy Object> Object Access** container.<br>3. Check the effective settings for Audit policy and compare with the following settings. | | | |
| 1. | Audit Policy: Object Access: File-System | Defines whether the audit is activated when file objects are accessed. | No auditing |
| 2. | Audit Policy: Object Access: Registry | Defines whether the audit is activated when registry objects are accessed. | No auditing |

| # | Setting Name | Description | Suggested Setting |
|---|---|---|---|
| The path to configure the following settings is as below.<br>1. Click **Start > Run** and type **gpedit.msc**.<br>2. Expand **Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration > System Audit Policy – Local Group Policy Object> Privilege Use** container.<br>3. Check the effective settings for Audit policy and compare with the following settings. | | | |
| 1. | Audit Policy: Privilege Use: Sensitive Privilege Use | Defines whether the audit is activated when a user account or service uses a sensitive privilege. | No auditing<br><br>Note: For critical system servers, enable both 'Success and Failure'. |
| The path to configure the following settings is as below.<br>1. Click **Start > Run** and type **gpedit.msc**.<br>2. Expand **Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration > System Audit Policy – Local Group Policy Object> Detailed Tracking** container.<br>3. Check the effective settings for Audit policy and compare with the following settings. | | | |
| 1. | Audit Policy: Detailed Tracking: Process Creation | Defines whether the audit is activated when a process is created and the name of the program that created it. | Success |
| The path to configure the following settings is as below.<br>1. Click **Start > Run** and type **gpedit.msc**.<br>2. Expand **Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration > System Audit Policy – Local Group Policy Object> Policy Change** container.<br>3. Check the effective settings for Audit policy and compare with the following settings. | | | |
| 1. | Audit Policy: Policy Change: Audit Policy Change | Defines whether the audit is activated when change in audit policy including SACL changes occur. | Success and Failure |
| 2. | Audit Policy: Policy Change: Authentication Policy Change | Defines whether the audit is activated when changes in the authentication policy occur. | Success |
| The path to configure the following settings is as below.<br>1. Click **Start > Run** and type **gpedit.msc**.<br>2. Expand **Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy** | | | |

| # | Setting Name | Description | Suggested Setting |
|---|---|---|---|
| **Configuration > System Audit Policy – Local Group Policy Object> Account Management** container.<br>3. Check the effective settings for Audit policy and compare with the following settings. | | | |
| 1. | Audit Policy: Account Management: Computer Account Management | Defines whether the audit is activated when a computer account management event, such as create, change, rename, delete, disable or enable event occurs. | Success<br>Note: For critical system servers, enable both 'Success and Failure'. |
| 2. | Audit Policy: Account Management: Other Account Management Events | Defines whether the audit is activated when an account management event occurs. | Success<br>Note: For critical system servers, enable both 'Success and Failure'. |
| 3. | Audit Policy: Account Management: Security Group Management | Defines whether the audit is activated when a security group management event, such as create, change or delete event occurs. | Success<br>Note: For critical system servers, enable both 'Success and Failure'. |
| 4. | Audit Policy: Account Management: User Account Management | Defines whether the audit is activated when a user account management event, such as create, change, rename, delete, disable or enable event occurs. | Success<br>Note: For critical system servers, enable both 'Success and Failure'. |
| The path to configure the following settings is as below.<br>1. Click **Start > Run** and type **gpedit.msc**.<br>2. Expand **Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration > System Audit Policy – Local Group Policy Object> DS Access** container.<br>3. Check the effective settings for Audit policy and compare with the following settings. | | | |
| 1. | Audit Policy: DS Access: Directory Service Access | Defines whether the audit is activated when an AD DS object is accessed. | No auditing – Member Server<br>Success and Failure – Domain Controller |
| 2. | Audit Policy: DS Access: Directory Service Changes | Defines whether the audit is activated when changes in Active Directory Domain Services occur. | No auditing – Member Server |

| # | Setting Name | Description | Suggested Setting |
|---|---|---|---|
| | | | Success and Failure – Domain Controller |
| The path to configure the following settings is as below.<br>1. Click **Start > Run** and type **gpedit.msc**.<br>2. Expand **Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration > System Audit Policy – Local Group Policy Object> Account Logon** container.<br>3. Check the effective settings for Audit policy and compare with the following settings. | | | |
| 1. | Audit Policy: Account Logon: Credential Validation | Defines whether the audit is activated to report the results of validation tests on credentials submitted by a user account logon request. | Success – Member Server<br><br>Success and Failure – Domain Controller |

| Title | 22.Weak user rights |
|---|---|
| ***Description*** | User rights are typically assigned on the basis of the security groups to which a user belongs, such as Administrators, Power Users or Users. |
| ***Risk Rating*** | High |

**Impact:** Malicious user can modify system configuration leading to non-availability of system and unauthorized access to critical data.

**Solution:**

1. Click **Start > Run** and type **gpedit.msc**.
2. Expand **Computer Configuration > Windows Settings > Security Settings > Local Policies/Domain Security Policy/Domain Controller Security Policy > User Rights Assignment** container
3. Check the effective settings for User Rights Assignment and compare with the following table:

**Note:**

1. Before changing the user rights assignment the administrator should take the backup of the current user rights assignment as follows:

- ✓ Go to **Start > Programs > Administrative Tools > Local/Domain Security Policy/Domain Controller Security Policy.**
- ✓ Right click on the "**User Rights Assignment**" entity on the left panel.
- ✓ Select "**Export List**" from the drop down window.
- ✓ Select the location on the local system and save the service settings.
- ✓ Use the Change Tracking Sheet in Appendix 1 to track all the changes.

1. Followings are the broader user rights. The administrator needs to review each user right and assign to the corresponding users group as per their environment. A low privilege users group other than the suggested users group can be assigned against the corresponding user right. However it is recommended not to assign a high privilege users group against the corresponding user right until & unless required by your specific operating environment.

2. **Not defined** setting means that the item does not impact a system's security configuration as the guideline does not recommend a specific value for that setting.

| # | Policy | Description | Suggested Setting | |
|---|---|---|---|---|
| | | | Enterprise Member Server Policy | Enterprise Domain Controller Policy |
| 1. | Access this computer from the network | Determines which users are allowed to connect over the network to the computer. | ✓ Administrators<br>✓ Authenticated Users<br>✓ Administrators | ✓ uthenticated Users<br>✓ NTERPRIS |

| # | Policy | Description | Suggested Setting | |
|---|---|---|---|---|
| | | | Enterprise Member Server Policy | Enterprise Domain Controller Policy |
| | | | | E D O M A I N C O N T R O L L E R S |
| 1. | Act as part of the operating system | It allows a process to perform as a secure, trusted part of the operating system. The process will impersonate any user without | ✓ No one | ✓ o o |

| # | Policy | Description | Suggested Setting | |
|---|---|---|---|---|
| | | | Enterprise Member Server Policy | Enterprise Domain Controller Policy |
| | | authentication thus gaining access to the same local resources as that user. The potential access is not limited to what is associated with the user by default; rather the process can have any and all accesses. | | ne |
| 1. | Add workstations to domain | It allows a user to add a computer to a specific domain. | ✓ Not Defined | ✓ dministrators |
| 1. | Adjust memory quota for a process | It determines who can change the maximum memory that can be consumed by a process. | ✓ Not defined | ✓ otdefined |

| # | Policy | Description | Suggested Setting | |
|---|---|---|---|---|
| | | | Enterprise Member Server Policy | Enterprise Domain Controller Policy |
| 1. | Allow log on locally | It determines which users can interactively log on to this computer. Logons initiated by pressing CTRL+ALT+DEL sequence on the attached keyboard requires the user to have this logon right. | ✓ Administrators | ✓ dministrators |
| 1. | Allow log on through Terminal Services | This security setting determines which users or groups have permission to log on as a Terminal Services client. | ✓ Administrators | ✓ dministrators |
| 1. | Back up files and directories | It allows the user to circumvent file and directory permissions to backup the system. | ✓ Not defined | ✓ otdef |

| # | Policy | Description | Suggested Setting | |
|---|---|---|---|---|
| | | | Enterprise Member Server Policy | Enterprise Domain Controller Policy |
| | | | | ined |
| 1. | Bypass traverse checking | Allows the user to traverse through folders without listing the folder contents to which the user otherwise has not access while navigating an object path in any Microsoft Windows file system or in the Registry. | ✓ Administrators<br>✓ Authenticated Users<br>✓ Backup Operators<br>✓ Local Service<br>✓ Network Service | ✓ otdefined |
| 1. | Change the system time | Allows the user to set the time for the internal clock of the computer. | ✓ Administrators<br>✓ Local Service | ✓ dministrators<br>✓ oc |

| # | Policy | Description | Suggested Setting | |
|---|---|---|---|---|
| | | | Enterprise Member Server Policy | Enterprise Domain Controller Policy |
| | | | | al Service |
| 1. | Create a pagefile | Allows the user to create and change the size of a pagefile. | ✓ Administrators | ✓ ot defined |
| 1. | Create a token object | Allows a user to create an access token by calling NtCreateToken() or other token creating APIs. | ✓ No one | ✓ oone |
| 1. | Create global objects | Allows a user to create global objects that are available to all sessions. | ✓ Not defined | ✓ otdef |

| # | Policy | Description | Suggested Setting | |
|---|---|---|---|---|
| | | | Enterprise Member Server Policy | Enterprise Domain Controller Policy |
| | | | | ined |
| 1. | Create permanent shared objects | Allows a process to create a directory object in the Windows 2008 object manager. This privilege is useful to kernel-mode components that extend the Windows 2008 object namespace. Components that are running in kernel mode already have this privilege; it is not necessary to assign it to them. | ✓ No one | |
| 1. | Debug programs | Allows the user to attach a debugger to any process. | ✓ Not defined | ✓ otdefined |
| 1. | Deny access to this computer from the network | Prohibits a user or group from connecting to the computer from the network. | ✓ Guests | ✓ uest |

| # | Policy | Description | Suggested Setting | |
|---|---|---|---|---|
| | | | Enterprise Member Server Policy | Enterprise Domain Controller Policy |
| | | | | s |
| 1. | Deny logon as a batch job | Prohibits a user or group from logging on through a batch-queue facility. | ✓ Guests | ✓ u e st s |
| 1. | Deny log on as a service | Prohibits a user or group from logging on as a service. | ✓ No One<br>Note: **No One** means no user or group should be added under this setting. | ✓ o O n e<br>N ot e : **N o O** |

| # | Policy | Description | Suggested Setting | |
|---|---|---|---|---|
| | | | Enterprise Member Server Policy | Enterprise Domain Controller Policy |
| | | | | **ne** means no user or groups sho |

| # | Policy | Description | Suggested Setting | |
|---|---|---|---|---|
| | | | Enterprise Member Server Policy | Enterprise Domain Controller Policy |
| | | | | uld be added under this setting. |
| 1. | Deny logon locally | Prohibits a user or group from logging on locally | ✓ Guests | ✓ |

| # | Policy | Description | Suggested Setting | |
|---|---|---|---|---|
| | | | Enterprise Member Server Policy | Enterprise Domain Controller Policy |
| | | at the keyboard. | | uests |
| 1. | Enable computer and user accounts to be trusted for delegation | In a domain controller it allows the user to change the Trusted for Delegation setting on a user or computer in Active Directory. The user or computer that is granted this privilege must also have write access to the account control flag on the object. | ✓ No One<br>Note: **No One** means no user or group should be added under this setting. | ✓ oOne<br>Note: **NoOne** means |

| # | Policy | Description | Suggested Setting | |
|---|---|---|---|---|
| | | | Enterprise Member Server Policy | Enterprise Domain Controller Policy |
| | | | | no user or group should be added u |

| # | Policy | Description | Suggested Setting | |
|---|---|---|---|---|
| | | | Enterprise Member Server Policy | Enterprise Domain Controller Policy |
| | | | | nder this setting. |
| 1. | Force shutdown from a remote system | Allows a user to shut down a computer from a remote location on the network. | ✓ Not defined | ✓ ot Defined |
| 1. | Generate security audits | Allows a process to generate entries in the security log. The security log is used to trace | ✓ Network Service<br>✓ Local Service | ✓ ot defi |

| # | Policy | Description | Suggested Setting | |
|---|---|---|---|---|
| | | | Enterprise Member Server Policy | Enterprise Domain Controller Policy |
| | | unauthorized system access and other security relevant activities. | | ned |
| 1. | Impersonate a client after authentication | Assigning this privilege to a user allows programs running on behalf of that user to impersonate a client. | ✓ Administrators<br>✓ SERVICE<br>✓ Network Service<br>✓ Local Service | ✓ dmi nist rato rs<br>✓ ERV ICE<br>✓ etw ork Ser vice<br>✓ ocal Ser vice |
| 1. | Increase scheduling priority | Allows a process that has Write Property access to another process to increase the execution | ✓ Not defined | ✓ ot |

| # | Policy | Description | Suggested Setting | |
|---|---|---|---|---|
| | | | Enterprise Member Server Policy | Enterprise Domain Controller Policy |
| | | priority of the other process. | | defined |
| 1. | Load and unload device drivers | Allows a user to install and uninstall Plug & Play device drivers. This privilege does not apply to device drivers that are not Plug & Play; only Administrators can install these device drivers.<br><br>Device drivers run as Trusted (highly privileged) processes.<br><br>A user can abuse this privilege by installing hostile programs and giving them destructive access to resources. | ✓ Administrators | ✓ dministrators |
| 1. | Lock pages in memory | Allows a process to keep data in physical memory, which prevents the system from paging data to virtual memory on disk. Assigning this privilege can result in significant degradation of system performance. | ✓ Not defined | ✓ ot defined |
| 1. | Log on as a batch job | Allows the user to log on by using the batch-queue facility. | ✓ Not Defined | ✓ o One |

| # | Policy | Description | Suggested Setting | |
|---|---|---|---|---|
| | | | Enterprise Member Server Policy | Enterprise Domain Controller Policy |
| | | | | Note: **No One** means no user or group should be added under this setting. |
| 1. | Log on as a service | Determines under which user context services | ✓ Not defined | ✓ ot |

| # | Policy | Description | Suggested Setting | |
|---|---|---|---|---|
| | | | Enterprise Member Server Policy | Enterprise Domain Controller Policy |
| | | are executed (Log On As). Services mostly execute under Local System account which has a built-in right to log on as a service. | | defined |
| 1. | Manage auditing and security log | Determines which users can specify object access auditing options for individual resources, like files, Active Directory objects & registry keys. Object access auditing is not actually performed unless it has been enabled in the Audit Policy. A user who has this privilege also can view and clear the security log from event viewer. | ✓ Administrators | ✓ ot defined |
| 1. | Modify firmware environment values | Allows modification of system environment variables either by a process through an API or by a user through the System Properties applet. | ✓ Administrators | ✓ ot defined |
| 1. | Perform volume maintenance tasks | It determines which users & groups can run maintenance tasks on a volume, such as remote defragmentation. | ✓ Not defined | ✓ ot defi |

| # | Policy | Description | Suggested Setting | |
|---|---|---|---|---|
| | | | Enterprise Member Server Policy | Enterprise Domain Controller Policy |
| | | | | ned |
| 1. | Profile single process | Determines which user can use performance monitoring tools to monitor the performance of non system processes. | ✓ Administrators | ✓ dministrators |
| 1. | Profile system performance | Determines which user can use performance monitoring tools to monitor the performance of system processes. | ✓ Administrators | ✓ dministrators |
| 1. | Remove computer from docking station | Allows a user to undock a portable computer from its docking station without logging on. | ✓ Administrators<br>✓ Power Users<br>✓ Users | ✓ dministrators |
| 1. | Replace a process level token | Allows a parent process to change the access token associated with a child process. | ✓ Local Service<br>✓ Network Service | ✓ ocal Service<br>✓ |

| # | Policy | Description | Suggested Setting | |
|---|---|---|---|---|
| | | | Enterprise Member Server Policy | Enterprise Domain Controller Policy |
| | | | | etwork Service |
| 1. | Restore files and directories | Determines which users can bypass file, directory, registry and other persistent object permissions when restoring backed up files and directories.<br>Determines which users can set any valid security principal as the owner of an object. | ✓ Administrators<br>✓ Backup Operators | ✓ dministrators<br>✓ ackup Operators |
| 1. | Shut down the system | Determines which users who are logged on locally to the computer can shut down the operating system using the Shut Down command. | ✓ Administrators | ✓ dministrators |

| # | Policy | Description | Suggested Setting | |
|---|---|---|---|---|
| | | | Enterprise Member Server Policy | Enterprise Domain Controller Policy |
| 1. | Synchronize directory service data | Determines which users and groups have the authority to use Active Directory Synchronization (synchronization of all directory service data) | ✓ No One<br>Note: **No One** means no user or group should be added under this setting. | ✓ o One<br>Note: **No One** means no user or group should be added under this setting. |
| 1. | Take ownership of files or | Allows the user to take ownership of any | ✓ Administrators | ✓ |

| # | Policy | Description | Suggested Setting | |
|---|---|---|---|---|
| | | | Enterprise Member Server Policy | Enterprise Domain Controller Policy |
| | other objects | securable object in the system, including Active Directory objects, files, folders, printers, registry keys, processes & threads. | | dmi nistr ator s |
| 1. | Change the time zone | Allows the user to change the time zone of a computer. | ✓ Local Service<br>✓ Administrators | ✓ ocal Serv ice<br>✓ dmi nistr ator s |
| 1. | Create symbolic links | Allows a user to create a symbolic links on the system. | ✓ Not defined | ✓ ot defi ned |
| 1. | Deny logon through Terminal Service | Prohibits a user from logging on as Terminal Service client. | ✓ Guests | ✓ uest s |

| # | Policy | Description | Suggested Setting | |
|---|---|---|---|---|
| | | | Enterprise Member Server Policy | Enterprise Domain Controller Policy |
| 1. | Increase a process working set | Determines whether a user is allowed to increase or decrease the size of a process's working set – the set of memory pages currently visible on the process in the physical RAM memory. | ✓ Not defined | ✓ ot defi ned |
| 1. | Access credential Manager as a trusted caller | Defines whether a user is allowed to access user credentials though the Credential Manager. | ✓ No One<br>Note: **No One** means no user or group should be added under this setting. | ✓ o One<br>Note : **No One** mea ns no user or grou p shou ld be adde d und |

| # | Policy | Description | Suggested Setting | |
|---|---|---|---|---|
| | | | Enterprise Member Server Policy | Enterprise Domain Controller Policy |
| | | | | er this setti ng. |

| Title | 23. Incorrect configuration of security options |
|---|---|
| *Description* | Windows 2008 platform has explicit security parameters that can be configured. |
| *Risk Rating* | High |

**Impact:** Malicious user can modify critical system information leading to non-availability of system, unauthorized access to critical data.

**Solution:**

1. Click **Start > Run** and type **gpedit.msc**.
2. Expand **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options** container.
3. Check the effective settings for Security Options and compare with the following table:

**Note:**

1. Before changing the security option settings the administrator should take the backup of the current security option settings as follows:

✓ Go to **Start > Programs > Administrative Tools > Local / Domain Security Policy / Domain Controller Security Policy.**

✓ Right click on the "**Security Options**" entity on the left panel.

✓ Select "**Export List**" from the drop down window.

✓ Select the location on the local system and save the service settings.

✓ Use the Change Tracking Sheet in Appendix 1 to track all the changes.

1. Followings are the broader Security Options Setting. The administrator needs to review each Security Option and enable or disable as per their specific environment.

| # | Policy | Description | Suggested Setting |
|---|---|---|---|
| | | | Enterprise Member Server Policy |
| 1. | Accounts: Administrator Account Status | It enables or disables the Administrator account during the normal operation. | ✓ Not defined |
| 1. | Accounts: Guest account status | Determines whether Guest account is enabled or disabled. This account allows unauthenticated users to log on as Guest and gain access to the computer. | ✓ Disabled |
| 1. | Accounts: Limit local | Determines whether local accounts that are not | ✓ Enabled |

| # | Policy | Description | Suggested Setting<br>Enterprise Member Server Policy |
|---|---|---|---|
| | account use of blank passwords to console logon only | password protected can be used to log on from locations other than the physical computer console. When the setting is enabled, the computer refuses remote logons if the user attempts to use a blank password, even if the blank password is valid for that account. | |
| 1. | Accounts: Rename administrator account | Determines whether a different account name will be associated with the security identifier (SID) for the account "Administrator". By associating Administrator SID with another account, you will no longer have the account named "Administrator", which is often a point of attack by hackers. | ✓ Any value that does not contain the term "admin". |
| 1. | Accounts: Rename guest account | Determines whether a different account name will be associated with the security identifier (SID) for the account "Guest". By associating Guest SID with another account, you will no longer have the account named "Guest", which is often a point of attack by hackers. | ✓ Any value that does not contain the term "guest". |
| 1. | Audit: Audit the access of global system objects | Determines whether access of global system objects (e.g. Mutexes, events, semaphores etc) will be audited or not. | ✓ Not defined |
| 1. | Devices: Allow undock without having to log on | Determines whether a portable computer can be undocked without the user having to log on to the computer. When enabled this policy eliminates the logon requirement and allows the use of an external hardware eject button to undock the computer.<br>Note:<br>If this policy is disabled, a user who is not logged on must be assigned the "Remove computer from docking station" user right. | ✓ Disabled |
| 1. | Devices: Allowed to format and eject removable media | Determines who can format and eject removable media. | ✓ Administrators |
| 1. | Devices: Prevent users | Determines whether the member of the users group is | ✓ Enabled |

| # | Policy | Description | Suggested Setting<br>Enterprise Member Server Policy |
|---|---|---|---|
| | from installing printer drivers | prevented from installing printer drivers.<br>When printer drivers are installed onto an operating system, their code is installed directly into the privilege space of the operating system kernel. This allows printer drivers to accomplish tasks that are beyond the actual user's capability. Further it can lead the operating system to execute malicious code in the form of "Trojan Horse" printer driver. | |
| 1. | Devices: Restrict CD-ROM access to locally logged-on user only | Determines whether a CD-ROM is accessible to both local and remote users simultaneously.<br>If enabled, this policy allows only the interactively logged-on user to access the removable CD-ROM media. If no one is logged on interactively, the CD-ROM may be shared over the network.<br>**Note:**<br>When users are installing software from a CD-ROM drive that uses Microsoft Installer packages (.msi), the software is installed by Windows Installer service, and not the local user. If this setting is enabled, such software installation will not be able to proceed, because of this restriction. Alternatively the package must be copied to a local or network drive for the installation procedure to succeed. | ✓ Not Defined |
| 1. | Devices: Restrict floppy access to locally logged-on user only | Determines whether removable floppy media is accessible to both local and remote users simultaneously.<br>If enabled, this policy allows only the interactively logged-on user to access the removable floppy media. If no one is logged on interactively, the floppy media may be shared over the network. | ✓ Not defined |
| 1. | Domain controller: Allow server operators to schedule tasks | Determines whether members of the Server Operators group are allowed to submit jobs by means of the AT schedule facility (by default AT runs under the local | ✓ Not defined |

| # | Policy | Description | Suggested Setting<br>Enterprise Member Server Policy |
|---|---|---|---|
| | | system account, which has the administrative privileges).<br><br>When the setting is disabled, Server Operators can still schedule tasks with the task scheduler; however these tasks will run under their domain credentials and not under the local system account. | |
| 1. | Domain controller: LDAP server signing requirements | Determines whether the LDAP server requires a signature before it will negotiate with LDAP clients.<br><br>**Note:**<br><br>LDAP signing requires Windows 2003, Windows XP, and Windows 2000 SP 3. | ✓ Not Defined |
| 1. | Domain controller: Refuse machine account password changes | This setting will allow to domain to prevent the computer from changing the computer account password. If the policy is enabled on all the domain controllers in a domain, computer account passwords on domain members will not be able to be changed and they will be more susceptible to attacks. | ✓ Not Defined |
| 1. | Domain member: Digitally encrypt or sign secure channel data (always) | Determines whether the computer will always digitally encrypt or sign secure channel data.<br><br>When a Windows 2008 system joins a domain, a computer account is created. Thereafter when the system boots, it uses the password for that account to create a secure channel with the domain controller in its domain. Requests sent on the secure channel are authenticated, and sensitive information (such as password) is encrypted. But the channel is not integrity checked and not all information is encrypted.<br><br>If this policy is enabled, all outgoing secure channel traffic must be either encrypted or signed.<br><br>If the computer is unable to connect to a DC by a signed or encrypted channel, no session will be established. | ✓ Enabled |

| # | Policy | Description | Suggested Setting<br>Enterprise Member Server Policy |
|---|---|---|---|
| 1. | Domain member: Digitally encrypt secure channel data (when possible) | Determines whether the computer will digitally encrypt the secure channel data.<br>If this policy is enabled, all outgoing secure channel traffic should be encrypted whenever possible. | ✓ Enabled |
| 1. | Domain member: Digitally sign secure channel data (when possible) | Determines whether the computer will digitally sign the secure channel data.<br>If this policy is enabled, all outgoing secure channel traffic should be signed whenever possible. | ✓ Enabled |
| 1. | Domain member: Disable machine account password changes | Determines whether a domain member may periodically change its computer account password. If the policy is enabled, the domain member will not be able to change its computer account password. If it is disabled, the domain member will be able to change its computer account password as specified by the "Domain member: Maximum machine account password age" setting. | ✓ Disabled |
| 1. | Domain member: Maximum machine account password age | Determines the maximum allowable age for a computer account password. By default, the domain members automatically change their domain passwords every 30 days. | ✓ 30 day(s) |
| 1. | Domain member: Require strong (Windows 2000 or later) session key | This setting applies specifically to the netlogon secure channel established between workstations and domain controllers (see security option 18). This setting only impacts workstations which have joined a domain.<br>By default, workstations will accept a weak 64-bit session key to encrypt the secure channel. However this setting allows the workstation to require a strong 128-bit session key for the secure channel.<br>**Note:**<br>Only enable this setting if all the domain controllers support 128-bit encrypted secure channel (Windows 2000 SP 4 & later) | ✓ Enabled |

| # | Policy | Description | Suggested Setting<br>Enterprise Member Server Policy |
|---|---|---|---|
| 1. | Interactive Logon: Do not display last user name in logon screen | Determines whether the name of the last user to logon to the computer is displayed in the Windows logon screen.<br>Anyone who walks up to a computer and presses CTRL+ALT+DEL can see the name of the last valid user who logged on to that system. As a result, they now have the name of a valid user for that computer. | ✓ Enabled |
| 1. | Interactive Logon: Do not require CTRL+ALT+DEL | Determines whether pressing CTRL+ALT+DEL is required before a user can log on.<br>If this policy is enabled on a computer, a user is not required to press CTRL+ALT+DEL before logon; ensures that the user is commuCDACating by means of a trusted path when entering their password. | ✓ Disabled |
| 1. | Interactive Logon: Message text for users attempting to log on | Specifies a text message that is displayed to users when they log on.<br>This text is often used for legal reasons, such as to warn users about the ramifications of misusing company information or to warn them that their actions may be audited. | ✓ Any text message as per the organization policy. |
| 1. | Interactive Logon: Message title for users attempting to log on | Allows the specification of a title to appear in the title bar of the windows that contains the message text for users attempting to log on. | ✓ Any text message as per the organization policy. |
| 1. | Interactive Logon: Number of previous logons to cache | This policy determines whether a user can log on to a Windows domain with cached account information. Logon information for domain accounts can be cached locally so that if a domain controller cannot be contacted on subsequent logons, a user can still log on. This capability might allow users to log on after their account has been disabled or deleted, because the workstation does not contact the domain controller. | ✓ 0 logons |
| 1. | Interactive Logon: Prompt user to change password | Determines how many days in advance users are warned that their passwords are about to expire. | ✓ 14 days |

| # | Policy | Description | Suggested Setting<br>Enterprise Member Server Policy |
|---|---|---|---|
| | before expiration | | |
| 1. | Interactive Logon: Require domain controller authentication to unlock workstation | For domain accounts, this policy setting determines whether a domain controller must be contacted to unlock a computer. If this is disabled, then a user could disconnect the network cable of the server, unlock the server with an old password, and unlock the server without authentication. | ✓ Enabled |
| 1. | Interactive Logon: Require Smart card | This policy setting requires users to log on to a computer with a smart card. | ✓ Not Defined |
| 1. | Interactive Logon: Smart card removal behavior | Determines what should happen when a smart card for a logged-on user is removed from the smart card reader.<br>The options are:<br>1. No Action<br>2. Lock Workstation<br>3. Force Logoff | ✓ Lock Workstation |
| 1. | Microsoft network client: Digitally sign commuCDACations (always) | This policy setting determines whether packet signing is required by the SMB client component. | ✓ Enabled |
| 1. | Microsoft network client: Digitally sign commuCDACations (if server agrees) | This policy determines whether SMB client will attempt to negotiate SMB packet signatures. If the policy is enabled, the Microsoft network clients on member servers will request signatures only if the servers with which they commuCDACate accept digitally signed commuCDACation. | ✓ Enabled |
| 1. | Microsoft network client: Send unencrypted password to connect to third-party SMB servers | If this policy is enabled, the SMB redirector is allowed to send clear-text password to non-Microsoft SMB servers, which do not support password encryption during authentication. | ✓ Disabled |
| 1. | Microsoft network server: | The policy setting determines the amount of continuous | ✓ 15 minute(s) |

| # | Policy | Description | Suggested Setting<br>Enterprise Member Server Policy |
|---|---|---|---|
| | Amount of idle time required before suspending session | idle time that must pass in an SMB session before the session is suspended because of inactivity. Administrators can use this policy setting to control when a computer suspends an inactive SMB session. If client activity resumes, the session is automatically reestablished. | |
| 1. | Microsoft network server: Digitally sign commuCDACations (always) | If the policy is enabled, it always requires the windows 2008 SMB server to perform SMB packet signing; however any situation that prevents it will prevent the session entirely. | ✓ Enabled |
| 1. | Microsoft network server: Digitally sign commuCDACations (if client agrees) | If this policy is enabled, it causes the Windows 2008 SMB server to perform SMB packet signing whenever possible. If not possible, for whatever reason, the server commuCDACation will not be signed, but commuCDACation will be permitted. | ✓ Enabled |
| 1. | Microsoft network server: Disconnect clients when logon hours expire | This policy setting determines whether to disconnect users who are connected to a network computer outside of their user account's valid logon hours. This policy setting affects the SMB component. If logon hours have been configured for users, then it makes sense to enable this policy setting. Otherwise, users should not be able to access network resources outside of their logon hours or they may be able to continue to use those resources with sessions that were established during allowed hours. | ✓ Enabled |
| 1. | Network access: Allow anonymous SID/name translation | This policy setting determines whether an anonymous user can request SID attributes for another user. If this policy setting is enabled, a user with local access could use the well-known Administrators SID to obtain the real name of the built-in Administrator account, even if the account has been renamed. That person could then use the account to initiate a password guessing attack. | ✓ Disabled |
| 1. | Network access: Do not allow anonymous | This policy setting determines what additional permissions will be granted to anonymous connection to | ✓ Enabled |

| # | Policy | Description | Suggested Setting<br>Enterprise Member Server Policy |
|---|---|---|---|
| | enumeration of SAM accounts | the computer. Windows allows anonymous users to perform certain activities, such as enumerate the names of domain accounts. However, even if this setting is enabled, anonymous user can still access resources that have permission that explicitly include the built-in account ANONYMOUS LOGON. | |
| 1. | Network access: Do not allow anonymous enumeration of SAM accounts and shares | This policy setting determines whether anonymous enumeration of SAM accounts and shares is allowed. | ✓ Enabled |
| 1. | Network access: Do not allow storage of credentials or .NET passports for network authentication | This policy setting determines whether settings for *Stored Username and Password* will save passwords, credentials or Microsoft .NET passports for later use after domain authentication is achieved. | ✓ Not Defined |
| 1. | Network access: Let Everyone permission apply to anonymous users | This policy setting determines what additional permissions are granted to anonymous connections to the computer. If it is enabled anonymous Windows will be able to perform certain activities, such as enumerate the names of domain accounts and network shares. | ✓ Disabled |
| 1. | Network access: Named pipes that can be accessed anonymously | This policy setting determines which commuCDACation sessions (named pipes) will have attributes and permissions that allow anonymous access.<br>The default values consists of the following pipes:<br>1. COMNAP – SNA session access<br>2. COMNODE – SNA session access<br>3. SQL\QUERY – SQL instance access<br>4. SPOOLSS – Spooler service<br>5. LLSRPC – License Logging service<br>6. Netlogon – Net Logon service<br>7. Lsarpc – LSA access<br>8. Samr – SAM access<br>9. browser – Computer Browser service | ✓ Not Defined |

| # | Policy | Description | Suggested Setting<br>Enterprise Member Server Policy |
|---|---|---|---|
| 1. | Network access: Remotely accessible registry paths | Determines whether registry paths can be accessed over the network.<br>**Note:**<br>Even if this policy is configured, *Remote Registry Service* should be started if authorized users need to access the registry over the network. | ✓ System\CurrentControlSet\Control\ProductOptions<br>✓ System\CurrentControlSet\Control\Server Applications<br>✓ Software\Microsoft\WindowsNT\CurrentVersion |
| 1. | Network access: Remotely accessible registry paths and sub-paths | This policy determines which registry paths and sub-paths are accessible over the network. | ✓ Not defined |
| 1. | Network access: Restrict anonymous access to Named pipes and shares | This policy setting can be used to restrict anonymous access to shares and named pipes in the following setting:<br>1. Network access: Named pipes that can be accessed anonymously<br>2. Network access: Shares that can be accessed anonymously | ✓ Enabled |
| 1. | Network access: Shares that can be accessed anonymously | This policy setting determines which network shares can be accessed by anonymous users<br>**Note:**<br>This policy setting can be very dangerous, because any network user can access any shares that are listed. Sensitive data could be exposed or corrupted if this policy setting is enabled. | ✓ None |
| 1. | Network access: Sharing and security model for local accounts | Determines how Network logons using local accounts are authenticated. Following are the two models available:<br>1. Classic – Local users authenticate as themselves (allows different types of access to different users for the same resource).<br>2. Guest only – Local users authenticate as the | ✓ Classic |

| # | Policy | Description | Suggested Setting<br>Enterprise Member Server Policy |
|---|---|---|---|
| | | Guest account (all users receives the same access level to a given resource). | |
| 1. | Network security: Force logoff when logon hours expire | This security setting determines whether to disconnect users who are connected to the local computer outside their user account's valid logon hours. This setting affects the Server Message Block (SMB) component.<br>When this policy is enabled, it causes client sessions with the SMB server to be forcibly disconnected when the client's logon hours expire. | ✓ Not defined |
| 1. | Network security: Do not store LAN Manager hash value on next password change | Determines whether the LAN Manager (LM) hash value for the new password is stored when the password is changed.<br>**Note:**<br>Very old legacy operating systems and some applications may fail when this policy setting is enabled. Also, you will need to change the password on all accounts after this policy setting is enabled. | ✓ Enabled |
| 1. | Network security: LAN Manager Authentication Level | Determines which challenge/response authentication protocol is used for network logons.<br>Following are the possible values:<br>1. Send LM & NTLM responses - Clients use LM and NTLM authentication and never use NTLMv2 session security; domain controllers accept LM, NTLM, and NTLMv2 authentication.<br>2. Send LM & NTLM - use NTLMv2 session security if negotiated: Clients use LM and NTLM authentication and use NTLMv2 session security if the server supports it; domain controllers accept LM, NTLM, and NTLMv2 authentication.<br>3. Send NTLM response only - Clients use NTLM authentication only and use NTLMv2 session security if the server supports it; domain controllers accept LM, NTLM, and NTLMv2 authentication. | ✓ Send NTLMv2 responses only. refuse LM |

| # | Policy | Description | Suggested Setting<br>Enterprise Member Server Policy |
|---|---|---|---|
| | | 4. Send NTLMv2 response only - Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it; domain controllers accept LM, NTLM, and NTLMv2 authentication.<br>5. Send NTLMv2 response only\refuse LM - Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it; domain controllers refuse LM (accept only NTLM and NTLMv2 authentication).<br>6. Send NTLMv2 response only\refuse LM & NTLM - Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it; domain controllers refuse LM and NTLM (accept only NTLMv2 authentication). | |
| 1. | Network security: LDAP client signing requirements | This policy setting determines the level of data signing that is requested on behalf of clients that issue LDAP BIND requests. Unsigned network traffic is susceptible to man-in-the-middle attacks. For an LDAP server, an attacker could cause a server to make decisions that are based on false queries from the LDAP client. | ✓ Negotiate signing |
| 1. | Network security: Minimum session security for NTLM SSP based (including secure RPC) clients | This security setting allows a client to require the negotiation of message confidentiality (encryption), message integrity, 128-bit encryption, or NTLMv2 session security. These values are dependent on the LAN Manager Authentication Level security setting value.<br>1. Require message integrity - The connection will fail if message integrity is not negotiated. The integrity of a message can be assessed through message signing. Message signing proves that the message has not been tampered with by attaching a cryptographic signature which identifies the sender and is a numeric representation of the contents of the message. This signature ensures that the message has not been tampered with.<br>2. Require message confidentiality - The | ✓ Require NTLMv2 session security<br>✓ Require 128-bit encryption |

| # | Policy | Description | Suggested Setting<br>Enterprise Member Server Policy |
|---|---|---|---|
| | | connection will fail if encryption is not negotiated. Encryption converts data into a form that is not readable by anyone until decrypted.<br>3. Require NTLMv2 session security -The connection will fail if the NTLMv2 protocol is not negotiated.<br>4. Require 128-bit encryption - The connection will fail if strong encryption (128-bit) is not negotiated. | |
| 1. | Network security: Minimum session security for NTLM SSP based (including secure RPC) servers | This security setting allows a server to require the negotiation of message confidentiality (encryption), message integrity, 128-bit encryption, or NTLMv2 session security. These values are dependent on the LAN Manager Authentication Level security setting value.<br>1. Require message integrity - The connection will fail if message integrity is not negotiated. The integrity of a message can be accessed through message signing. Message signing proves that the message has not been tampered with by attaching a cryptographic signature which identifies the sender and is a numeric representation of the contents of the message. This signature ensures that the message has not been tampered with.<br>2. Require message confidentiality - The connection will fail if encryption is not negotiated. Encryption converts data into a form that is not readable by anyone until decrypted.<br>3. Require NTLMv2 session security -The connection will fail if the NTLMv2 protocol is not negotiated.<br>4. Require 128-bit encryption - The connection will fail if strong encryption (128-bit) is not negotiated. | ✓ Require NTLMv2 session security<br>✓ Require 128-bit encryption |
| 1. | Recovery Console: Allow automatic administrative logon | By default the Recovery console requires you to provide the password for the Administrator account before accessing the system. If this option is enabled then the Recovery Console does not require you to provide a | ✓ Disabled |

| # | Policy | Description | Suggested Setting<br>Enterprise Member Server Policy |
|---|---|---|---|
| | | password and will automatically log on to the system. | |
| 1. | Recovery Console: Allow floppy copy and access to all drives and all folders | Enabling this option enables the Recovery Console SET command, which allows you to set the following Recovery Console environment variables:<br>1. AllowWildChards – Enable wild character support for some commands (e.g. DEL command)<br>2. AllowAllPaths – Allow access to all files and folders on the computer.<br>3. AllowRemovableMedia – Allow files to be copied to removable media like floppy disks.<br>4. NoCopyPrompt – Do not prompt when copying an existing file. | ✓ Not defined |
| 1. | Shutdown: Allow system to be shut down without having to log on | Determines whether a computer can be shut down without having to log on. | ✓ Disabled |
| 1. | Shutdown: Clear virtual memory pagefile | Determines whether the virtual memory pagefile should be cleared when the system is shut down. | ✓ Disabled |
| 1. | System cryptography: Force strong key protection for user keys stored on the computer | This security setting determines if users' private keys require a password to be used. The options are:<br>1. User input is not required when new keys are stored and used<br>2. User is prompted when the key is first used<br>3. User must enter a password each time they use a key | ✓ User is prompted when the key is first used. |
| 1. | System cryptography: Use FIPS compliant algorithms for encryption, hashing & signing | FIPS (Federal Information Processing Standards) is a security implementation designed for certifying cryptographic software. Although the operating system can support a variety of hashing and encryption algorithms, only the followings are FIPS compliant:<br>1. Secure Hash Algorithm (SHG-1) for hashing<br>2. Triple Data Encryption Standard (DES) for encryption | ✓ Disabled |

| # | Policy | Description | Suggested Setting<br>Enterprise Member Server Policy |
|---|---|---|---|
| | | 3. Rivest, Shamir, and Adleman (RSA) for key exchange and authentication | |
| 1. | System objects: Require case insensitivity for non-Windows subsystems | This security setting determines whether case insensitivity is enforced for all subsystems. The Win32 subsystem is case insensitive. However, the kernel supports case sensitivity for other subsystems, such as POSIX. (Portable Operating System Interface for UNIX). Because Windows is case insensitive and the POSIX subsystem supports case sensitivity, failure to enforce this setting makes it possible for a POSIX user to create a file with the same name as another file if they use mixed case letters to label it. Such an occurrence may block another user's access to these files with typical Win32 tools, because only one of the files will be available. | ✓ Enabled |
| 1. | System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links) | Determines the strength of the default discretionary access control list (DACL) for objects, and helps secure objects that can be located and shared among processes.<br>If this policy is enabled, the default DACL is stronger, allowing users who are not administrators to read shared objects but not allowing these users to modify shared objects that they did not create. | ✓ Enabled |
| 1. | System settings: Optional subsystems | Determines which subsystems are used to support your applications. With this security setting, you can specify as many subsystems to support as your environment demands. | ✓ None<br>Note:<br>Add subsystems as required by your environment. |
| 1. | System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies | This policy setting determines whether digital certificates are processed when software restriction policies are enabled and a user or process attempts to run software with an .exe file name extension. It enables or disables certificate rules (a type of software restriction policies rule). With software restriction | ✓ Not defined |

| # | Policy | Description | Suggested Setting<br>Enterprise Member Server Policy |
|---|---|---|---|
| | | policies, you can create a certificate rule that will allow or disallow the execution of Authenticode®-signed software, based on the digital certificate that is associated with the software. For certificate rules to take effect in software restriction policies, you must enable this policy setting. | |

The followings settings which contain the prefix 'MSS' may not be visible in the Group Management Policy Editor.

i. To view these settings, please install **Microsoft Security Compliance Manager** and run **LocalGPO.msi**.

i. The Microsoft Security Compliance Manager(MSCM) can be downloaded from http://www.microsoft.com/en-us/download/details.aspx?id=16776

i. Once the MSCM is installed, traverse to the installation path of MSCM and locate the folder "LGPO". Under that folder, **LocalGPO.msi** is present. Run that file.

. Following that, please execute the command **Script LocalGPO.wsf /ConfigSCE** at the LocalGPO installation path.

| | | | |
|---|---|---|---|
| 1. | MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended) | Defines whether a user with physical access to the computer is able to automatically logon. | ✓ Disabled |
| 1. | MSS: (DisableIPSourcerouting) IP Source routing protection level (protects against packet spoofing) | Determines if Windows will accept source routed packets. Source routing allows the packet sender to dictate the route the packet will take to its destination. | ✓ Highest protection, source routing is completely disabled. |
| 1. | MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes | Defines whether the Internet Control Message Protocol (ICMP) redirects to override Open Shortest Path First (OSPF) generated routes. | ✓ Disabled |
| 1. | MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds | Defines every how many milliseconds TCP attempts to send a keep-alive packet to verify that an idle connection is still intact. | ✓ Not Defined |
| 1. | MSS: (NoDefaultExempt) Configure IPSec exemptions for various types of network | Defines whether IPSec exemptions could be configured for various type of network traffic such as Internet Key Exchange (IKE) and Kerberos | ✓ Only ISAKMP is exempt. |

| # | Policy | Description | Suggested Setting<br>Enterprise Member Server Policy |
|---|---|---|---|
| | traffic | authentication protocol. | |
| 1. | MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers. | Defines whether a computer disregards NetBIOS name release requests except those from WINS server in the SCE. | ✓ Enabled |
| 1. | MSS: (NtfsDisable8dot3NameCreation) Enable the computer to stop generating 8.3 style filenames | Defines whether a computer can stop generating 8.3 style file names. | ✓ Enabled |
| 1. | MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS) | Defines whether Internet Router Discovery Protocol (IRDP) is used to automatically detect and configure default gateway addresses. | ✓ Disabled |
| 1. | MSS: (SafeDllSearchMode) Enable Safe DLL search mode | Defines whether an application is forced to begin its DLL search in the system path before searching the current working folder. | ✓ Enabled |
| 1. | MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires | Defines how many seconds between when the screen saver is launched and when the computer console is actually locked. | ✓ 0 (zero) |
| 1. | MSS: (TCPMaxDataRetransmission) How many times unacknowledged data is retransmitted | Defines the number of times that TCP retransmits an individual data segment before the connection is aborted. | ✓ 3 |
| 1. | MSS: (WarningLevel) | It is the Percentage threshold for the security | ✓ 90% or less |

| # | Policy | Description | Suggested Setting<br>Enterprise Member Server Policy |
|---|---|---|---|
| | Percentage threshold for the security event log at which the system will generate a warning. | event log at which the system will generate a warning. | |
| 1. | MSS: (DisableIPSourceRouting IPv6) IP source routing protection level | Determines if Windows will accept source routed packets. | ✓ Highest protection, source routing is completely disabled. |
| 1. | MSS: (TCPMaxDataRetransmissions) IPv6 How many times unacknowledged data is retransmitted | Defines the number of times that TCP retransmits an individual data segment before the connection is aborted. | ✓ 3 |

| Title | 24. Inadequate space allocation for Event viewer |
|---|---|
| ***Description*** | All system-generated messages are logged and can be viewed using event viewer. |
| ***Risk Rating*** | Medium |

**Impact**: Critical logs might get overwritten in the absence of sufficient event viewer file size.

**Solution**:

1. Configure the Maximum Log Size

1.1.i. Click **Start** > **Run** and type **eventvwr.msc**.

1.1.ii. Expand **Windows logs** and Right click on **Application/ Security/ System**, choose the **Properties**.

1.1.iii. Check the **Maximum Log Size** as mentioned below.

1.1.iii.a) Application Log : 32,768 KB

1.1.iii.b) Security Log : 81,920 KB

1.1.iii.c) System Log : 32,768 KB

2. Retaining the old events: This control determines the event log behavior when the log file reaches the maximum log file size.

2.1.i. Click **Start** > **Run** and type **eventvwr.msc**.

2.1.ii. Expand **Windows logs** and Right click on **Application/ Security/ System**, choose the **Properties**.

2.1.iii. Enable '**Overwrite events as needed (oldest events first)**' under '**When maximum event log size is reached:**' setting.

**NOTE:** Further the security option - Audit: Shut down system immediately if unable to log security audits can be enabled to halt the system if a security audit cannot be logged for any reason.

| Title | 25.Shares with insecure permission |
|---|---|
| *Description* | Windows allows various access levels to be defined for users to system folders. Users can share folders and configure access permission for users and groups. |
| *Risk Rating* | High |

**Impact:** Malicious users can break weak share permissions and gain access to confidential data. Worms and viruses also use weak shares to propagate themselves in the network.

**Solution:** Restrict access on shares for specific users/groups with appropriate permissions.

**How to Check:**

1. Click Start > Run and type **compmgmt.msc**.
2. Expand **System Tools** > **Shared Folders** > **Shares** container
3. Double click on each and every custom created share name (except Admin$, IPC$, Print$, C$, D$, <Drive letter>$ etc.)
4. Go to **Share Permission** tab and check the permission for each user/group.

**Note:** An object's security descriptor may contain a discretionary access-control list (DACL). A DACL contains zero or more access-control entries (ACEs) that identify the users and groups who can access the object. If a DACL is empty (that is, it contains zero ACEs), no access is explicitly granted, so access is implicitly denied. However, if an object's security descriptor does not have a DACL, the object is unprotected and everyone has complete access.

| Title | 26.Weak permissions on critical system files |
|---|---|
| *Description* | Only Authorized users should be allowed to access critical files. **Everyone** group should never be permitted **FULL** access to critical system files. |
| *Risk Rating* | High |

**Impact:** Malicious user can modify critical system files leading to non-availability of system, unauthorized access to critical data.

**Solution:**

1. Restrict access on system files for specific users/groups with appropriate permissions.
2. Everyone group should not be configured with FULL control permission.

Only FULL control permission should be configured as given in the table below:

| Files / Directories | Full Control Permission |
|---|---|
| Audit logs | Administrator and System account |
| Repair (%systemroot%\repair) | Administrator and System account |
| Registry files (%systemroot%\system32\config) | Administrator and System account |
| Boot files on the system partition (Boot.ini, NTLDR, NTDETECT.COM) | Administrator and System account |
| System Root directory C:\WINDOWS or D:\WINDOWS | Administrator and System account |
| C:\ D:\ etc. | Everyone group should not be configured with full control permission |

| Title | **27.Auto play is enabled** |
|---|---|
| ***Description*** | Auto play on CD-ROM and other Drives is not configured by default during installation. Auto play feature of a CD-ROM or other drive presents a potential security threat by automatically running code when a CD is inserted into a machine. |
| ***Risk Rating*** | High |

**Impact:** Malicious code can be executed on a system automatically.

**Solution:**

1. Click **Start > Run** and type **gpedit.msc**.
2. Expand **Computer Configuration > Administrative Templates > Windows Components > AutoPlay Policies** container.
3. Select **Turnoff AutoPlay** setting and set **Enabled** option.

| Title | 28.Remote Registry Access is enabled |
|---|---|
| *Description* | Remote access to registry can be controlled through permission configuration at directory and registry level. |
| *Risk Rating* | High |

**Impact:** Registry manipulation using weak permissions can lead to system downtime and malicious access.

**Solution:**

Restrict access on registry for specific users/groups with appropriate permissions.

1. Click **Start** > **Run** and type **regedit**.
2. Go to the registry hive HKEY_LOCAL_MACHINE\System\CurrentcontrolSet\Control\SecurePipeServers\winreg\
3. Right Click on **Winreg** and select Permission. **FULL** Control should only be given to Administrators group & System Account.

| Title | 29.Critical Security patches are not installed |
|---|---|
| *Description* | Security patches provide bug fixes against latest vulnerabilities. |
| *Risk Rating* | High |

**Impact:** System can get affected by the latest vulnerabilities and can get compromised.

**Solution:**

1. Install the latest security patches for Windows 2008, IE 8, IIS, MSQL & any other installed component on the server.
2. Latest security patches are available for download from the following web site: http://www.microsoft.com/technet/security/current.aspx

| Title | 30. Incorrect setting of Recycle bin |
|---|---|
| ***Description*** | All deleted files are moved to the recycle bin. At times critical files that are deleted also remain in the recycle bin. |
| ***Risk Rating*** | Low |

**Impact**: An intruder can recover and access critical files.

**Solution**:

1. Users must be aware of clearing recycle bin on a regular basis to permanently delete files.
2. Right click on Recycle bin and click on properties.
3. Select the checkbox "Do not move files to the Recycle Bin. Remove files immediately when deleted".

| Title | 31. Incorrect setting of NTP server |
|---|---|
| ***Description*** | Many components of Microsoft Windows 2008 rely on accurate and synchronized time to function correctly. For example, with time synchronization, you can correlate events on different computers in an enterprise. With synchronized clocks on all of your computers, you ensure that you can correctly analyze events that happen in sequence on multiple computers. The Windows Time service automatically synchronizes a local computer's time with other computers on a network to improve security and performance in your organization. |
| ***Risk Rating*** | High |

**Impact:** Correlation of logs and establishment of timeline for any malicious activity detected cannot be accurately performed.

**Solution:**

The NTP server must be appropriately configured on the servers.

1. Click **Start** > **Run** and type **regedit**.
2. Go to the registry hive

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters

3. Set the following registry values:

| Registry Key Name | Type | Value |
|---|---|---|
| Type | REG_SZ | Used to control how a computer synchronizes. |

| Registry Key Name | Type | Value |
|---|---|---|
| | | Following are the possible values:<br>✓ Nt5DS (Synchronize to domain hierarchy)<br>✓ NTP (Synchronize to manually configured source)<br>✓ NoSync (Do not synchronize)<br>Default setting is Nt5DS<br>**Set the value as follows:**<br>✓ Domain Member Server – Nt5DS<br>✓ Non Domain Server – NTP (In this case NtpServer must be set to the IP Address or hostname of the system from which this system is expected to synchronize) |
| NtpServer | REG_SZ (optional for a Domain Member Server) | Used to manually configure the time source. This can be set to the DNS name or IP address of the server from which to synchronize. Only one DNS name or IP address can be specified.<br>Default setting is blank<br>Note: It must be set in case of a non domain server. |

# Appendix 1 : Hardening Guidelines for IIS 7.0

Following are the critical security guidelines for hardening IIS 7.0 on a production system:

1 Web-Content should be kept on Non-System Partition

2 Default folders like AdminScripts, IISSamples, IISHelp, msadc, printers etc. should be removed

3 Default Application Pool Identity should be set to least privilege identity

4 Application Pools should Run Under Unique Identities

5 There should be Unique Application Pools for Sites

6 Only strong encryption protocols (SSL 3.0 or TLS 1.x) should be used

7 Weak Cipher Suites (DES 56/56, NULL cipher, RC2 40/128 etc.) should be disabled. Instead stronger cipher suite like AES should be used

8 If Basic Authentication is being used then SSL should be configured with Basic Authentication

9 Debugging should be off

10 Custom error messages should be enabled

11 Session state should be configured to "Use Cookies Mode"

12 Cookies should be set with HttpOnly Attribute

13 Request Filtering should be enabled

14 HTTP Trace Method should be disabled

15 IIS Advanced Logging should be enabled in W3C format (IIS Advanced Logging is a module which provides flexibility in logging requests and client). Further at-least the following fields should be logged:

a. *date*

b. *time*

c. *s-ip*

d. *cs-method*

e. *cs-uri-stem*

f. *cs-uri-query*

g. *s-port*

h. *c-ip*

i. *cs(User-Agent)*

j. *cs(Referer)*

k. *sc-status*

l. *sc-bytes*

16 FTP Requests should be encrypted

# Appendix 2 : Change Tracking Sheet

## Service Tracking Sheet

| # | Full Service Name | Current Setting | | New Setting |
|---|---|---|---|---|
| | Alerter | **Status** | **Startup Type** | **Status** |
| 1. | Alerter | Started<br>Stopped | Automatic<br>Manual<br>Disabled | Started<br>Stopped |
| 2. | ClipBook | Started<br>Stopped | Automatic<br>Manual<br>Disabled | Started<br>Stopped |
| 3. | Cluster Service | Started<br>Stopped | Automatic<br>Manual<br>Disabled | Started<br>Stopped |
| 4. | DHCP Client | Started<br>Stopped | Automatic<br>Manual<br>Disabled | Started<br>Stopped |
| 5. | DHCP Server | Started<br>Stopped | Automatic<br>Manual<br>Disabled | Started<br>Stopped |

| # | Full Service Name | Current Setting | | New Setting |
|---|---|---|---|---|
| | Alerter | **Status** | **Startup Type** | **Status** |
| 6. | Distributed File System | Started<br>Stopped | Automatic<br>Manual<br>Disabled | Started<br>Stopped |
| 7. | Distributed Link Tracking Server | Started<br>Stopped | Automatic<br>Manual<br>Disabled | Started<br>Stopped |
| 8. | DNS Server | Started<br>Stopped | Automatic<br>Manual<br>Disabled | Started<br>Stopped |
| 9. | Fax Service | Started<br>Stopped | Automatic<br>Manual<br>Disabled | Started<br>Stopped |
| 10. | File Replication | Started<br>Stopped | Automatic<br>Manual<br>Disabled | Started<br>Stopped |
| 11. | File Server for Macintosh | Started<br>Stopped | Automatic<br>Manual<br>Disabled | Started<br>Stopped |
| 12. | FTP Publishing Service | Started<br>Stopped | Automatic<br>Manual<br>Disabled | Started<br>Stopped |
| 13. | IIS Admin Services | Started<br>Stopped | Automatic<br>Manual<br>Disabled | Started<br>Stopped |
| 14. | Indexing Service | Started<br>Stopped | Automatic<br>Manual | Started<br>Stopped |

| # | Full Service Name | Current Setting | | New Setting |
|---|---|---|---|---|
| | Alerter | **Status** | **Startup Type** | **Status** |
| | | | Disabled | |
| 15. | Internet Connection Sharing | Started<br>Stopped | Automatic<br>Manual<br>Disabled | Started<br>Stopped |
| 16. | Messenger | Started<br>Stopped | Automatic<br>Manual<br>Disabled | Started<br>Stopped |
| 17. | NetMeeting Remote Desktop Sharing | Started<br>Stopped | Automatic<br>Manual<br>Disabled | Started<br>Stopped |
| 18. | Network DDE | Started<br>Stopped | Automatic<br>Manual<br>Disabled | Started<br>Stopped |
| 19. | Network DDE DSDM | Started<br>Stopped | Automatic<br>Manual<br>Disabled | Started<br>Stopped |
| 20. | Network News Transfer Protocol(NNTP) | Started<br>Stopped | Automatic<br>Manual<br>Disabled | Started<br>Stopped |
| 21. | Print Server for Macintosh | Started<br>Stopped | Automatic<br>Manual<br>Disabled | Started<br>Stopped |
| 22. | Print Spooler | Started<br>Stopped | Automatic<br>Manual<br>Disabled | Started<br>Stopped |

| # | Full Service Name | Current Setting | | New Setting |
|---|---|---|---|---|
| | Alerter | **Status** | **Startup Type** | **Status** |
| 23. | Remote Access Auto Connection Manager | Started<br>Stopped | Automatic<br>Manual<br>Disabled | Started<br>Stopped |
| 24. | Remote Registry | Started<br>Stopped | Automatic<br>Manual<br>Disabled | Started<br>Stopped |
| 25. | Remote Storage Server | Started<br>Stopped | Automatic<br>Manual<br>Disabled | Started<br>Stopped |
| 26. | Removable Storage | Started<br>Stopped | Automatic<br>Manual<br>Disabled | Started<br>Stopped |
| 27. | Routing and Remote Access | Started<br>Stopped | Automatic<br>Manual<br>Disabled | Started<br>Stopped |
| 28. | Simple Mail Transport Protocol (SMTP) | Started<br>Stopped | Automatic<br>Manual<br>Disabled | Started<br>Stopped |
| 29. | Smart Card | Started<br>Stopped | Automatic<br>Manual<br>Disabled | Started<br>Stopped |
| 30. | SNMP Service | Started<br>Stopped | Automatic<br>Manual<br>Disabled | Started<br>Stopped |
| 31. | SNMP Trap Service | Started<br>Stopped | Automatic<br>Manual | Started<br>Stopped |

| # | Full Service Name | Current Setting | | New Setting |
|---|---|---|---|---|
| | Alerter | **Status** | **Startup Type** | **Status** |
| | | | Disabled | |
| 32. | Telnet | Started<br>Stopped | Automatic<br>Manual<br>Disabled | Started<br>Stopped |
| 33. | Terminal Services | Started<br>Stopped | Automatic<br>Manual<br>Disabled | Started<br>Stopped |
| 34. | World Wide Web Publishing Service | Started<br>Stopped | Automatic<br>Manual<br>Disabled | Started<br>Stopped |

## Account Policies

| Policy | Current Setting | New Setting |
|---|---|---|
| **Password Policy** | | |
| Enforce Password History | | |
| Maximum Password Age | | |
| Minimum Password Age | | |
| Minimum Password Length | | |
| Passwords Must Meet Complexity Requirements | | |
| Store Password Using Reversible Encryption | | |

| Policy | Current Setting | New Setting |
|---|---|---|
| **Account Lockout Policy** | | |
| Account Lockout Duration | | |
| Account Lockout Threshold | | |
| Reset Account Lockout Threshold After | | |
| **Kerberos Policy** | | |
| Enforce user logon restrictions | | |
| Maximum tolerance for computer clock synchronization | | |
| Maximum lifetime for service ticket | | |
| Maximum lifetime for user ticket renewal | | |
| Maximum lifetime for user ticket | | |

## Audit Policy

| Policy | Current Setting | New Setting |
|---|---|---|
| Audit: Shut down system immediately if unable to log security audits | No auditing<br>Success<br>Failure | No auditing<br>Success<br>Failure |
| Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit. | No auditing<br>Success<br>Failure | No auditing<br>Success<br>Failure |
| Audit Policy: System: IPSec Driver | No auditing<br>Success<br>Failure | No auditing<br>Success<br>Failure |
| Audit Policy: System: Security State Change | No auditing<br>Success | No auditing<br>Success |

| Policy | Current Setting | New Setting |
|---|---|---|
| | Failure | Failure |
| Audit Policy: System: Security State Extension | No auditing<br>Success<br>Failure | No auditing<br>Success<br>Failure |
| Audit Policy: System: System Integrity | No auditing<br>Success<br>Failure | No auditing<br>Success<br>Failure |
| Audit Policy: Logon-Logoff: Logoff | No auditing<br>Success<br>Failure | No auditing<br>Success<br>Failure |
| Audit Policy: Logon-Logoff: Logon | No auditing<br>Success<br>Failure | No auditing<br>Success<br>Failure |
| Audit Policy: Logon-Logoff: Special Logon | No auditing<br>Success<br>Failure | No auditing<br>Success<br>Failure |
| Audit Policy: Object Access: File-System | No auditing<br>Success<br>Failure | No auditing<br>Success<br>Failure |
| Audit Policy: Object Access: Registry | No auditing<br>Success<br>Failure | No auditing<br>Success<br>Failure |
| Audit Policy: Privilege Use: Sensitive Privilege Use | No auditing<br>Success<br>Failure | No auditing<br>Success<br>Failure |
| Audit Policy: Detailed Tracking: Process Creation | No auditing<br>Success<br>Failure | No auditing<br>Success<br>Failure |
| Audit Policy: Policy Change: Audit Policy Change | No auditing<br>Success | No auditing<br>Success |

| Policy | Current Setting | New Setting |
|---|---|---|
| | Failure | Failure |
| Audit Policy: Policy Change: Authentication Policy Change | No auditing<br>Success<br>Failure | No auditing<br>Success<br>Failure |
| Audit Policy: Account Management: Computer Account Management | No auditing<br>Success<br>Failure | No auditing<br>Success<br>Failure |
| Audit Policy: Account Management: Other Account Management Events | No auditing<br>Success<br>Failure | No auditing<br>Success<br>Failure |
| Audit Policy: Account Management: Security Group Management | No auditing<br>Success<br>Failure | No auditing<br>Success<br>Failure |
| Audit Policy: Account Management: User Account Management | No auditing<br>Success<br>Failure | No auditing<br>Success<br>Failure |
| Audit Policy: DS Access: Directory Service Access | No auditing<br>Success<br>Failure | No auditing<br>Success<br>Failure |
| Audit Policy: DS Access: Directory Service Changes | No auditing<br>Success<br>Failure | No auditing<br>Success<br>Failure |
| Audit Policy: Account Logon: Credential Validation | No auditing<br>Success<br>Failure | No auditing<br>Success<br>Failure |

## User Rights Tracking Sheet

| # | User Right | Current Setting (User/Groups) | New Setting (User/Groups) |
|---|---|---|---|
| 1. | Access this computer from the network | | |
| 2. | Act as part of the operating system | | |
| 3. | Add workstations to domain | | |
| 4. | Adjust memory quota for a process | | |
| 5. | Allow log on locally | | |
| 6. | Allow log on through Terminal Services | | |
| 7. | Back up files and directories | | |
| 8. | Bypass traverse checking | | |
| 9. | Change the system time | | |

| # | User Right | Current Setting (User/Groups) | New Setting (User/Groups) |
|---|---|---|---|
| 10. | Create a pagefile | | |
| 11. | Create a token object | | |
| 12. | Create global objects | | |
| 13. | Create permanent shared objects | | |
| 14. | Debug programs | | |
| 15. | Deny access to this computer from the network | | |
| 16. | Deny logon as a batch job | | |
| 17. | Deny log on as a service | | |
| 18. | Deny logon locally | | |
| 19. | Enable computer and user accounts to be trusted for delegation | | |

| # | User Right | Current Setting (User/Groups) | New Setting (User/Groups) |
|---|---|---|---|
| 20. | Force shutdown from a remote system | | |
| 21. | Generate security audits | | |
| 22. | Impersonate a client after authentication | | |
| 23. | Increase scheduling priority | | |
| 24. | Load and unload device drivers | | |
| 25. | Lock pages in memory | | |
| 26. | Log on as a batch job | | |
| 27. | Log on as a service | | |
| 28. | Manage auditing and security log | | |
| 29. | Modify firmware environment values | | |

| # | User Right | Current Setting (User/Groups) | New Setting (User/Groups) |
|---|---|---|---|
| 30. | Perform volume maintenance tasks | | |
| 31. | Profile single process | | |
| 32. | Profile system performance | | |
| 33. | Remove computer from docking station | | |
| 34. | Replace a process level token | | |
| 35. | Restore files and directories | | |
| 36. | Shut down the system | | |
| 37. | Synchronize directory service data | | |
| 38. | Take ownership of files or other objects | | |
| 39. | Change the time zone | | |

| # | User Right | Current Setting (User/Groups) | New Setting (User/Groups) |
|---|---|---|---|
| 40. | Create symbolic links | | |
| 41. | Deny logon through Terminal Service | | |
| 42. | Increase a process working set | | |
| 43. | Access credential Manager as a trusted caller | | |

## Security Options Tracking Sheet

| # | Policy | Current Setting | New Setting |
|---|---|---|---|
| 1. | Accounts: Administrator Account Status | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 2. | Accounts: Guest account status | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 3. | Accounts: Limit local account use of blank passwords to console logon only | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 4. | Accounts: Rename administrator account | | |
| 5. | Accounts: Rename guest account | | |
| 6. | Audit: Audit the access of global system objects | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 7. | Devices: Allow undock without having to log on | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 8. | Devices: Allowed to format and eject removable media | Administrators<br>Administrators and Power Users<br>Administrators and Interactive Users | Administrators<br>Administrators and Power Users<br>Administrators and Interactive Users |
| 9. | Devices: Prevent users from installing printer drivers | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 10. | Devices: Restrict CD-ROM access to locally logged-on user only | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 11. | Devices: Restrict floppy access to locally logged-on user only | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 12. | Domain controller: Allow server operators to schedule tasks | Enabled<br>Disabled | Enabled<br>Disabled |

| # | Policy | Current Setting | New Setting |
|---|---|---|---|
| | | Not defined | Not defined |
| 13. | Domain controller: LDAP server signing requirements | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 14. | Domain controller: Refuse machine account password changes | Silently succeed<br>Warn but allow installation<br>Do not allow installation | Silently succeed<br>Warn but allow installation<br>Do not allow installation |
| 15. | Domain member: Digitally encrypt or sign secure channel data (always) | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 16. | Domain member: Digitally encrypt secure channel data (when possible) | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 17. | Domain member: Digitally sign secure channel data (when possible) | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 18. | Domain member: Disable machine account password changes | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 19. | Domain member: Maximum machine account password age | | |
| 20. | Domain member: Require strong (Windows 2000 or later) session key | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 21. | Interactive Logon: Do not display last user name in logon screen | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 22. | Interactive Logon: Do not require CTRL+ALT+DEL | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 23. | Interactive Logon: Message text for users attempting to log on | | |
| 24. | Interactive Logon: Message | | |

| # | Policy | Current Setting | New Setting |
|---|---|---|---|
| | title for users attempting to log on | | |
| 25. | Interactive Logon: Number of previous logons to cache | | |
| 26. | Interactive Logon: Prompt user to change password before expiration | | |
| 27. | Interactive Logon: Require domain controller authentication to unlock workstation | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 28. | Interactive Logon: Require Smart card | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 29. | Interactive Logon: Smart card removal behavior | No Action<br>Lock Workstation<br>Force Logoff | No Action<br>Lock Workstation<br>Force Logoff |
| 30. | Microsoft network client: Digitally sign commuCDACations (always) | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 31. | Microsoft network client: Digitally sign commuCDACations (if server agrees) | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 32. | Microsoft network client: Send unencrypted password to connect to third-party SMB servers | No Action<br>Lock Workstation<br>Force Logoff | No Action<br>Lock Workstation<br>Force Logoff |
| 33. | Microsoft network server: Amount of idle time required before suspending session | | |
| 34. | Microsoft network server: Digitally sign commuCDACations (always) | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |

| # | Policy | Current Setting | New Setting |
|---|---|---|---|
| 35. | Microsoft network server: Digitally sign commuCDACations (if client agrees) | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 36. | Microsoft network server: Disconnect clients when logon hours expire | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 37. | Network access: Allow anonymous SID/name translation | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 38. | Network access: Do not allow anonymous enumeration of SAM accounts | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 39. | Network access: Do not allow anonymous enumeration of SAM accounts and shares | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 40. | Network access: Do not allow storage of credentials or .NET passports for network authentication | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 41. | Network access: Let Everyone permission apply to anonymous users | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 42. | Network access: Named pipes that can be accessed anonymously | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 43. | Network access: Remotely accessible registry paths | | |
| 44. | Network access: Remotely accessible registry paths and sub-paths | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 45. | Network access: Restrict anonymous access to Named | Enabled<br>Disabled | Enabled<br>Disabled |

| # | Policy | Current Setting | New Setting |
|---|---|---|---|
| | pipes and shares | Not defined | Not defined |
| 46. | Network access: Shares that can be accessed anonymously | | |
| 47. | Network access: Sharing and security model for local accounts | Classic<br>Guest only | Classic<br>Guest only |
| 48. | Network security: Force logoff when logon hours expire | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 49. | Network security: Do not store LAN Manager hash value on next password change | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 50. | Network security: LAN Manager Authentication Level | Send LM & NTLM responses<br>Send LM & NTLM responses, use NTLMv2 session security if negotiated<br>Send NTLMv2 response only<br>Send NTLMv2 response only\refuse LM<br>Send NTLMv2 response only\refuse LM & NTLM | Send LM & NTLM responses<br>Send LM & NTLM responses, use NTLMv2 session security if negotiated<br>Send NTLMv2 response only<br>Send NTLMv2 response only\refuse LM<br>Send NTLMv2 response only\refuse LM & NTLM |
| 51. | Network security: LDAP client signing requirements | None<br>Negotiate signing<br>Require signing | None<br>Negotiate signing<br>Require signing |
| 52. | Network security: Minimum session security for NTLM SSP based (including secure RPC) clients | Require message integrity<br>Require message confidentiality<br>Require NTLMv2 session security<br>Require 128-bit encryption | Require message integrity<br>Require message confidentiality<br>Require NTLMv2 session security<br>Require 128-bit encryption |
| 53. | Network security: Minimum session security for NTLM SSP based (including secure RPC) servers | Require message integrity<br>Require message confidentiality<br>Require NTLMv2 session security<br>Require 128-bit encryption | Require message integrity<br>Require message confidentiality<br>Require NTLMv2 session security<br>Require 128-bit encryption |
| 54. | Recovery Console: Allow automatic administrative logon | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 55. | Recovery Console: Allow floppy copy and access to all drives | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |

| # | Policy | Current Setting | New Setting |
|---|---|---|---|
| | and all folders | | |
| 56. | Shutdown: Allow system to be shut down without having to log on | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 57. | Shutdown: Clear virtual memory pagefile | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 58. | System cryptography: Force strong key protection for user keys stored on the computer | User input is not required when new keys are stored and used<br>User is prompted when the key is first used<br>user must enter a password each time they use a key<br>Not defined | User input is not required when new keys are stored and used<br>User is prompted when the key is first used<br>user must enter a password each time they use a key<br>Not defined |
| 59. | System cryptography: Use FIPS compliant algorithms for encryption, hashing & signing | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 60. | System objects: Require case insensitivity for non-Windows subsystems | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 61. | System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links) | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 62. | System settings: Optional subsystems | | |
| 63. | System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies | Administrators group<br>Object creator<br>Not defined | Administrators group<br>Object creator<br>Not defined |
| 64. | MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended) | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 65. | MSS: (DisableIPSourcerouting) IP Source routing protection | No additional protection, source packets are allowed | No additional protection, source packets are allowed |

| # | Policy | Current Setting | New Setting |
|---|---|---|---|
| | level (protects against packet spoofing) | Medium, source routed packets ignored when IP forwarding is enabled<br>Highest protection, source routing is completely disabled | Medium, source routed packets ignored when IP forwarding is enabled<br>Highest protection, source routing is completely disabled |
| 66. | MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 67. | MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 68. | MSS: (NoDefaultExempt) Configure IPSec exemptions for various types of network traffic | Allow all exemptions (least secure)<br>Multicast, broadcast, & ISAKMP exempt (best for Windows XP)<br>RSVP, Kerberos, and ISAKMP are exempt.<br>Only ISAKMP is exempt (recommended for Windows Server 2003) | Allow all exemptions (least secure)<br>Multicast, broadcast, & ISAKMP exempt (best for Windows XP)<br>RSVP, Kerberos, and ISAKMP are exempt.<br>Only ISAKMP is exempt (recommended for Windows Server 2003) |
| 69. | MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers. | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 70. | MSS: (NtfsDisable8dot3NameCraetion) Enable the computer to stop generating 8.3 style filenames | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 71. | MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS) | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 72. | MSS: (SafeDllSearchMode) Enable Safe DLL search mode | Enabled<br>Disabled<br>Not defined | Enabled<br>Disabled<br>Not defined |
| 73. | MSS: (ScreenSaverGracePeriod) The | | |

| # | Policy | Current Setting | New Setting |
|---|---|---|---|
| | time in seconds before the screen saver grace period expires | | |
| 74. | MSS: (TCPMaxDataRetransmission) How many times unacknowledged data is retransmitted | | |
| 75. | MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning. | 50%<br>60%<br>70%<br>80%<br>90% | 50%<br>60%<br>70%<br>80%<br>90% |
| 76. | MSS: (DisableIPSourceRouting IPv6) IP source routing protection level | No additional protection, source packets are allowed<br>Medium, source routed packets ignored when IP forwarding is enabled<br>Highest protection, source routing is completely disabled | No additional protection, source packets are allowed<br>Medium, source routed packets ignored when IP forwarding is enabled<br>Highest protection, source routing is completely disabled |
| 77. | MSS: (TCPMaxDataRetransmissions) IPv6 How many times unacknowledged data is retransmitted | | |

## Permission on shared objects

| # | Shared Folder | Shared Path | Settings |
|---|---|---|---|
| | | | Current Setting |
| 1. | | | Full Control<br>Change<br>Read |
| 2. | | | Full Control<br>Change<br>Read |

| # | Shared Folder | Shared Path | Settings |
|---|---|---|---|
| | | | Current Setting |
| 3. | | | Full Control<br>Change<br>Read |
| 4. | | | Full Control<br>Change<br>Read |
| 5. | | | Full Control<br>Change<br>Read |
| 6. | | | Full Control<br>Change<br>Read |
| 7. | | | Full Control<br>Change<br>Read |
| 8. | | | Full Control<br>Change<br>Read |
| 9. | | | Full Control<br>Change<br>Read |
| 10. | | | Full Control<br>Change<br>Read |

## Permission on critical system files

| # | Files / Directories | Current Setting | | New Setting |
|---|---|---|---|---|
| | | Users / Groups | Permission | Users / Groups |
| 1. | | | | |
| 2. | | | | |
| 3. | | | | |
| 4. | | | | |
| 5. | | | | |
| 6. | | | | |
| 7. | | | | |
| 8. | | | | |
| 9. | | | | |
| 10. | | | | |
| 11. | | | | |
| 12. | | | | |
| 13. | | | | |

| # | Files/Directories | Current Setting | New Setting |
|---|---|---|---|
| 14. | | | |

## Appendix 2: References

| # | Reference | Link |
|---|---|---|
| 1. | Windows Server 2008 TechCDACal Library | http://technet.microsoft.com/en-us/library/dd349801%28v=ws.10%29 > Secure Windows Server |
| 2. | Windows Server 2008 Security Guide | http://technet.microsoft.com/en-us/library/cc514539.aspx |
| 3. | Center for Internet Security – Windows 2008 Benchmarks | http://benchmarks.cisecurity.org/en-us/?route=downloads.show.single.windows2008.110 |

**CONTRIBUTED BY:**

1. Mr Ch A.S Murty
2. Mr Tyeb Naushad
3. Mr Devi Satish
4. Mr Shrinath Rusia
5. Ms Vertika Singh
6. Mr Vinay Kumar

**C-DAC, Hyderabad**

www.
InfoSec
awareness.in

**For any queries on Information Security**
**Call us on Tollfree No:**

**1800 425 6235**

**Between 10 A M TO 6 P M**
**Or give us a missed call, we will cal back within 24 hrs**

सत्यमेव जयते

Department of Electronics & Information Technology
Ministry of Communications & Information Technology
Government of India

सी डैक
CDAC
www.cdac.in

प्रगत संगणन विकास केन्द्र
**CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING**
संचार एवं सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Communications and Information Technology, Government of India
Plot No. 6 & 7, Hardware Park, Sy No. 1/1, Srisailam Highway,
Pahadi Shareef Via Keshavagiri (Post), Hyderabad - 500005, Telangana(India)