CERT-In Security Guideline CISG-2003-09

CERT-In

Indian Computer Emergency Response Team

Handling Computer Security Incidents

Microsoft Windows 2000 Advanced Server Security Guidelines

Department of Information Technology
Ministry of Communications and Information Technology
Govt. of India

Issue Date: October 21, 2003

Table of Contents

1. Physical Security

Physical security of domain controllers/servers is very important. Access to the domain controllers/ should be limited to only authorised persons. Physical security ensures that unauthorized users cannot power the domain controller on or off, add or remove hardware, insert or remove removable media, log on by using the domain controller's keyboard and display, or remove backup media.

To maintain physical security for domain controllers:

- Secure domain controllers against physical access.
- Prevent domain controllers from booting into alternate operating systems.
- Protect domain controllers on restart by using SYSKEY.
- Secure backup media against physical access.
- Enhance the security of the network infrastructure.
- Secure the remote restart of domain controllers.

1.1 Securing Domain Controllers against Physical Access

The first line of defense in maintaining physical security is to secure domain controllers against any attacks that can be accomplished with physical access to the domain controller. Following steps can be taken for restricting physical access to the domain controller:

- Use UPSs to prevent loss of power
- Place domain controllers and UPSs in a locked room
- Require cardkey locks on the entrances to the locked room
- Require locks on individual domain controllers or on doors to the racks housing the domain controllers
- Require specific processes and procedures for any administration or repair of the domain controllers

1.2 Prevent Domain Controllers from Booting into Alternate Operating Systems

Domain controller can be booted into an alternate operating system. For example, public domain drivers exist for MS-DOS that an attacker can use to boot the domain controller and directly access files that are stored on NTFS disk volumes, bypassing existing NTFS permissions. You can take steps to avoid this type of attack.

To minimize the possibility of having domain controllers boot into an alternate operating system:

- Disable or remove the floppy disk drive, unless it is required by SYSKEY
- Disable or remove the CD-ROM/DVD drive.
- Set the [timeout] parameter in the boot.ini file to 0.
- Disable remote network boot and installation, for example, by RIS or BOOTP.
- In case SYSKEY with a password or floppy disk is not used, require a BIOS password to boot the computer.

1.3 Protect Domain Controllers on Restart by Using SYSKEY

The system key (SYSKEY) in Windows 2000 protects security information, including passwords in the Active Directory database and other Local Security Authority (LSA) secrets, against offline attacks by encrypting their storage on the domain controller.

SYSKEY can either be derived from a secret password that you specify, or it can be stored on offline media, such as a floppy disk. On a domain controller reboot, either the password or the floppy disk containing SYSKEY must be supplied to successfully restart the computer.

1.4 Secure Backup Media Against Physical Access

As part of normal operational practices, SA should regularly back up domain controllers/servers and secure the backup media to minimize the risk of data tampering or theft. Since the backup contains all the information in the Active Directory database, theft of the backup media presents the same risks as theft of the domain controller or a disk drive from the domain controller. The attacker could restore the information elsewhere and illegally access Active Directory data.

1.5 Enhance Security of Network Infrastructure

The placement of domain controllers in your environment directly affects the security of your domain controllers. The primary focus in network security is to isolate the domain controllers from unauthorized users while providing high-speed, secure access to authorized users. To ensure that domain controllers are properly isolated, secure any cabling rooms, and place domain controllers on secured network segments in your network.

2. Installation and Configuration

It is recommended that System Administrators (SAs) should first format the Server system and the begin installation of server software. Server installation process should be performed on a secure network segment or off the network until the security configuration is completed.

2.1 Patches & Security Updates

Time to time Microsoft releases various Patches for its operating systems and applications. These patches comprise service packs and hotfixes, which primarily are improvements and replacements to OS components. Security updates and hot fixes usually address some vulnerability that was discovered in common components of Windows or additional Microsoft applications. . Service Packs should be used in a test environment before installing on a production system, or at least wait until it has been released for a short while before installing it, and watch for industry feedback on the compatibility of that service pack.

It is important to be aware that Service Packs and Hotfixes are not just applicable to operating systems. Individual applications have their own Service Pack and Hotfix requirements. All the applications, if any, installed on the server should also be applied for the current service packs and hotfixes. Hotfixes are the intermediate updates to the operating systems released by the vendors before the service pack release. These updates are usually small and address a single problem. Hotfixes can be released within hours of discovery of any particular bug or vulnerability, because they address a single problem. Since they are normally released so quickly, they do not pass the rigorous testing involved with Service Packs. They should be used with caution at first, even more so than Service Packs. Always perform a backup of any critical files and create an Emergency Repair Disk (ERD) before performing any patching.

The patches can be downloaded from Microsoft's official website
http://www.microsoft.com

A command line tool is also available to automate the process of determining the hotfixes required for the system. This tool, called hfnetchk.exe, is located at
http://support.microsoft.com/default.aspx?scid=kb;EN-US;q303215

The tool can be used to check locally and remotely the status of patching on a Windows 2000 system. Multiple hotfixes can be applied in a batch file without rebooting between installations by using the Microsoft command-line QChain.exe tool. The tool is located at
http://support.microsoft.com/default.aspx?scid=kb;EN-US;q296861

Another tool qfecheck.exe can be used to track and verify installed hotfixes. The tool can be downloaded from
http://support.microsoft.com/default.aspx?scid=kb;en-us;Q282784

2.2 File System

It is recommended that NTFS5 be chosen over the file allocation table (FAT) file system and that the hard drive be formatted into two partitions for system and data areas. Microsoft released a new version of NTFS, called NTFS 5, which provides additional security features to the Windows file system. Windows NT 4.0 uses the older version of NTFS; therefore, within a mixed NT/Windows 2000 environment, any Windows NT 4.0 machine that wishes to see network shares on a Windows 2000 system, NTFS 5 partition must have installed Service Pack 4 or later.

2.3 Securing the File System Using ACLs

The default installation of File System should be secured by using Access Control List (ACL). After installation of Windows 2000 system additional steps should be taken concerning the file system access control mechanisms. In a default Windows 2000 installation 'Everyone' group has full access to root partitions. Remove Everyone group permission from all the root partitions. Appropriately apply 'Administrator' and 'System' group permissions. This action will ensure that anonymous users and guests have no access to the resource. In some isolated cases, the Everyone group may not be replaced as a result of application requirements, test the settings before deployment.

2.4 Restrict access to administrative tools and utilities

Windows 2000 provides many command line utilities to assist with the administration of the system. Access to these utilities is granted to all users by default. It is recommended that access to these utilities be restricted to Administrative Users. Examples of these utilities include cmd.exe, rpc.exe, regedt32.exe, and rexec.exe.

2.5 Disable default shares

Windows NT and Windows 2000 open hidden shares on each installation for use by the system account. (Typing NET SHARE from a command prompt can view all the shared folders on the system.) There are two ways to disable the default Administrative shares. One is to stop or disable the Server service, which removes the ability to share folders on the server. The other way is via the Registry by editing

HKeyLocalMachine\SYSTEM\CurrentControlSet\Services\LanManServer\ Parameters.

Edit AutoShareServer with a REG_DWORD Value of 0. Keep in mind that disabling these shares provide an extra measure of security, but may cause problems with applications. The changes should be tested in a lab environment before applying on the production system. The default-hidden shares are:

C$ D$ E$	Root of each partition. For a Windows 2000 Server, only members of the Administrators, Backup Operators and Server Operators group can connect to these shared folders.
ADMIN$	%SYSTEMROOT% This share is used by the system during remote administration of a computer. The path of this resource is always the path to the Windows 2000 system root (the directory in which Windows 2000 is installed: for example, C:\Winnt).
FAX$	On Windows 2000 server, this used by fax clients in the process of sending a fax. The shared folder temporarily caches files and accesses cover pages stored on the server.
IPC$	Temporary connections between servers using named pipes essential for communication between programs. It is used during remote administration of a computer and when viewing a computer's shared resources
NetLogon	This share is used by the Net Logon service of a Windows 2000 Server computer while processing domain logon requests.
PRINT$	%SYSTEMROOT%\SYSTEM32\SPOOL\DRIVERS Used during remote administration of printers.

2.6 Using Encrypted File System

EFS provides the core file encryption technology to store Windows NT file system (NTFS) files encrypted on disk. EFS is designed to address numerous concerns regarding the integrity of data stored on secondary storage within Windows 2000. EFS is designed to keep data private and unreadable to unauthorized users. With physical access, malicious users can boot a computer system into a file system other than NTFS effectively bypassing all security provided by NTFS, thus gaining access to all unencrypted files residing on the hard drive. EFS was designed to reduce the risks associated with mobile computing and unauthorized physical access through file encryption. EFS particularly addresses security concerns raised by tools available on other operating systems that allow users to access files from an NTFS volume without an access check. With EFS, data in NTFS files is encrypted on disk. The encryption technology used is public key-based and runs as an integrated system service making it easy to manage, difficult to attack, and transparent to the user. If a user attempting to access an encrypted NTFS file has the private key to that file, the user will be able to open the file and work with it transparently as a normal document. A user without the private key to the file is simply denied access. For maximum security, the EFS recovery certificate can be removed from the system after a successful backup by selecting the Delete Private Key if the Export is Successful checkbox.

2.7 Additional File System Security Settings

Additional steps should be taken to enhance the security of the file systems on Windows 2000 system that extend beyond ACLs and EFS. The Windows 2000 OS includes OS2 and Portable Operating System Interface for Computer Environment (POSIX) compliant environmental subsystems that allow Windows to run applications written for these operating systems. These resources should be removed unless they are necessary.

2.8 Remove OS2 and POSIX Subsystems

The Windows 2000 architecture includes applications programming interfaces (API) to emulate the OS2 and any POSIX-compliant OS. These features allow applications written for these Oss to be run on a Windows 2000 system. Because these subsystems can introduce vulnerabilities into a Windows 2000 system, it is recommended that they be removed. Removing the OS2 and POSIX subsystems is a two-step process: removing the subsystem executables and removing the subsystem registry keys. Windows 2000 stores backup copies of all running system DLLs in the %SystemRoot%\system32\dllcache folder. Successful manual removal of system files requires removal from two locations.

To remove all subsystem executables, delete the following files from
%SystemRoot%\dllcache folder:
os2.exe
os2ss.exe
os2srv.exe

Remove the following files from the %SystemRoot%system32 folder:
os2.exe
os2ss.exe
os2srv.exe
psxss.exe
posix.exe
To remove the subsystem registry entries, delete the following values from the *HKEY_LOCAL_MACHINE hive:*

- *\System \CurrentControlSet\Control\Session Manager\Environment\OS2LibPath*
- *\System \CurrentControlSet\Control\Session Manager\Subsystem \Optional*
- *\System \CurrentControlSet\Control\Session Manager\Subsystem \OS2*
- *\System \CurrentControlSet\Control\Session Manager\Subsystem \Posix*

These registry values contain information that pertains to locations and parameters for the OS2 and POSIX environmental subsystems. Once the subsystem binaries have been deleted, the values are no longer necessary.

2.9 Prevent Data Remnants

Data remnant is a concept where data remains accessible on a system even after it has been deleted. Windows 2000 has an invisible directory called Recycler, which is used to maintain a copy of data marked for deletion until it is permanently removed from the Recycle Bin. In a default configuration, the Windows 2000 virtual memory page file is not wiped clean during any type of system shutdown. Memory dumps can include passwords and other sensitive information, and it is recommended that they be disabled. The recycle bin contains a hidden directory RECYCLER that stores a copy of recently deleted files. The virtual memory page file should also be wiped clean on each system shutdown for the same reasons. A number of options introduce data remnant threats in an out-of-the-box configuration of Windows 2000 system.

2.10 Disable Dump file creation

A dump file can be a useful troubleshooting tool when either the system or application crashes and causes the infamous "Blue Screen of Death". However, they also can provide a hacker with potentially sensitive information such as application passwords. Dump file creation should be disabled through Control Panel. If needed to troubleshoot unexplained crashes at a later date, re-enable this option until the issue is resolved but be sure to disable it again later and delete any stored dump files.

2.11 Encrypt the Temp Folder

Applications use the temp folder to store copies of files while they are being updated or modified, but they don't always clean the folder when the program is closed. Encrypting the temp folder provides an extra layer of security for files.

2.12 Clear the Paging File at shutdown

The Pagefile is the temporary swap file Windows NT/2000 uses to manage memory and improve performance. However, some 3rd party programs may store unencrypted passwords in memory, and there may be other sensitive data cache as well. It is recommended to clear the pagefile at shutdown by editing the Registry Key **HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management** and changing the data value of the *ClearPageFileAtShutdown* value to 1

2.13 Hide the Domain Administrator Account

Every installation of Active Directory has an account named Administrator in each domain. This is the default administrative account, which is created during domain setup, the account is used to access and administer the directory service. This is a special account that the system protects to help ensure that it is available when needed. This account cannot be disabled or locked out.

The fact that this account is always created during domain setup, cannot be deleted, and cannot be disabled means that every malicious user who attempts to break into the system will assume that the account exists and that can it can be used as a target. For this reason, SA should rename it to something other than Administrator. When account is renamed, “Description” field for the account should also be changed acordingly. In addition, SA should create a decoy user account, called Administrator that has no special permissions or user rights.

3. Security Configuration

3.1 Securing Important system files

System files on the server system should protected against any break-in attack. When a remote executes some malaciuos coe, it tries to run windows system files like cmd.exe, net.exe, telnet.exe etc. At time of default installtion Everyone group has full access to windows system file folder, \winnt\system32\. All rights for the Everyone group, should be removed from the \winnt\system32 files

- arp.exe
- ipconfig.exe
- netstat.exe
- at.exe
- net.exe ?
- ping.exe
- cacls.exe
- nslookup.exe
- rdisk.exe
- cmd.exe
- posix.exe
- regedt32.exe
- debug.exe
- rcp.exe ?
- route.exe
- edit.com ?
- regedit.exe ?
- runone.exe
- edlin.exe ?
- rexec.exe
- syskey.exe
- finger.exe
- rsh.exe
- tracert.exe
- ftp.exe ?
- telnet.exe ?
- command.exe
- xcopy.exe ?
- nbtstat.exe

3.2 Establish Secure Domain Policy

Domain security policy settings provide Active Directory with domain-wide security options for handling authentication and authorization of Active Directory security principals. These policy settings are applied to all security principal accounts in the domain, unless inheritance is specifically blocked or overridden by another policy.

Domain Group Policy controls various categories of settings. To increase comprehensive security for the domain, apply the recommended password, account lockout, and Kerberos policy settings.

Domain policy settings are divided into multiple categories of settings. To increase comprehensive domain security:

- Establish password policy settings for domains
- Establish account lockout policy settings for domains
- Establish Kerberos policy settings for domains

3.2.1 Securing Password Policy Settings for Domains

In Windows 2000, the most common method for authenticating a user's identity is by the use of secret user passwords. Once a user has been identified and authenticated, the user can perform any tasks or access any resource for which he or she is authorized. Strong passwords generally enhance security for Active Directory users. Using strong passwords helps avoid the threat of an unauthorized user guessing (cracking) a weak password and acquiring the credentials of the compromised user account (spoofing). This is especially true for administrative accounts, because an unauthorized user could obtain administrative credentials and thus gain elevated privileges.

A complex password that changes regularly reduces the likelihood of a successful spoofing attack. Password policy settings control the complexity and lifetime for passwords. The default and recommended password policy settings for a domain are explained below.

Policy	Default	Recommended	Comments
Enforce password history	1 passwords	24 passwords	Prevents users from reusing passwords.
Maximum password age	42 days	(No change)	
Minimum password age	0 days	2 days	Prevents users from cycling through their password history to reuse passwords.
Minimum password length	0 characters	8 characters	Ensures minimum password strength.
Password must meet complexity requirements	Disabled	Enable	To make it difficult for password crackers
Store password using reverse encryption for all users in domain	Disabled	(No change)	

3.2.2 Securing Account Lockout Policy Settings for Domains

More than a few unsuccessful password tries during logon could represent an attacker's attempt to determine an account password by trial and error. Windows 2000 keeps track of logon attempts, and it can be configured to respond to this type of attack by disabling the account for a preset period of time. This is referred to as *account lockout*.

Account lockout policy settings control the threshold for this response and the actions to be taken once the threshold is reached.

Policy	Default	Recommended	Reason
Account lockout duration	Not defined	0 minutes	The value 0 means that after account lockout an Administrator is required to re-enable the account before account lockout reset has expired.
Account lockout threshold	0 tries	5 tries	The value 0 means that failed password tries never cause account lockout.
Reset account lockout counter after	Not defined	30 minutes	This setting protects against a sustained dictionary attack by imposing a nontrivial delay after 5 unsuccessful attempts. A higher value for this setting could result in increased help-desk calls for legitimate account lockouts.

3.2.3 Securing Kerberos Policy Settings for Domains

In Windows 2000, Kerberos provides the default mechanism for authentication services, as well as the authorization data necessary for a user to access a resource and perform a task on that resource. By reducing the lifetimes of Kerberos tickets, the risk of having a legitimate user's credentials stolen and successfully used by an attacker diminishes. However, authorization overhead increases.

Policy	Default	Recommended	Comments
Enforce user logon restrictions	Enabled	(No change)	A user must have the right to log on locally (for service on the same computer) or to access the service from the network.
Maximum lifetime for service ticket	600 minutes	(No change)	
Maximum lifetime for user ticket	10 hours	(No change)	
Maximum lifetime for user ticket renewal	7 days	(No change)	
Maximum tolerance for computer clock synchronization	5 minutes	(No change)	Maximum tolerance between the client's and server's clocks.

3.3 Secure Domain Controller Policy Settings

Domain controller policies are divided into multiple categories of settings. To enhance comprehensive security for the domain controllers:

- Establish domain controller user rights assignment policy settings
- Establish domain controller audit policy settings
- Establish domain controller security options policy settings
- Establish domain controller event log policy settings

3.3.1 Establish Domain Controller User Rights Assignment Policy Settings

User rights allow users to log on and perform specific administrative or operations tasks on the domain controllers. Ensure that the appropriate user rights are assigned to users in the domain so that the users can perform their intended functions without compromising the security of the domain controllers. Establish the policy settings for domain controller user rights assignment to properly limit the users who can log on to the domain controllers and perform the necessary administrative tasks.

The default and recommended settings for domain controller user rights assignment policies are shown below. All other user rights assignment policies are unchanged.

Policy	**Default Setting**	**Recommended Setting**	**Comments**
Log on locally	Administrators Backup Operators Account Operators Server Operators	Administrators Backup Operators Server Operators	Account Operators are for account management and have few (if any) reasons to log on locally.
Shut down the system	Administrators Backup Operators Account Operators Server Operators Print Operators	Administrators Backup Operators Server Operators	Account Operators and Print Operators have few (if any) reasons to shut down domain controllers.

3.3.2 Establish Domain Controller Audit Policy Settings

By default, Windows 2000 Active Directory does not configure any audit policy settings, and no Active Directory access or domain controller operation is audited in the default configuration. The recommendations presented here provide the minimum recommended security audit policy settings that you should configure to maintain an audit trail of security-sensitive operations.

Many possible objectives can be achieved by enabling audit policy, like intrusion detection or forensic analysis of security breaches. The primary goal of the security audit settings is to provide accountability for sensitive directory operations, including any administrative or configuration changes. When auditing for other reasons, such as intrusion detection, additional auditing may need to be enabled.

When auditing is enabled on the domain controllers, the number of events that are recorded in the Security event log increases. As a result, the maximum size of the Security event log must be increased.

Policy	**Default Setting**	**Recommended Setting**	**Comments**
Audit account logon events	No auditing	Success	Account logon events are generated when a domain user account is authenticated on a domain controller.
Audit account management	Not defined	Success	Account management events are generated when security principal accounts are created, modified, or deleted.
Audit directory service access	No auditing	Success	Directory services access events are generated when an Active Directory object with a system access control list (SACL) is accessed.
Audit logon events	No auditing	Success	Logon events are generated when a domain user interactively logs on to a domain controller or a network logon to a domain controller is performed to retrieve logon scripts and policies.
Audit object access	No auditing	(No change)	
Audit policy change	No auditing	Success	Policy change events are generated for changes to user rights assignment policies, audit policies, or trust policies.
Audit privilege use	No auditing	(No change)	
Audit process tracking	No auditing	(No change)	
Audit system events	No auditing	Success	System events are generated when a user restarts or shuts down the domain controller or when an event occurs that affects either the system security or the security log.

3.3.3 Establish Domain Controller Security Options Policy Settings

The default and recommended policy settings for domain controller security options are explained below.

Policy	Default Setting	Recommended Setting	Comments
Additional restrictions for anonymous connections	Not defined	None	
Allow Server Operators to schedule tasks (domain controllers only)	Not defined	Disabled	Restricts the individuals who can schedule tasks to Administrators, because scheduling usually runs as an elevated service.
Allow system to be shut down without having to log on	Not defined	Disabled	Requires an authenticated, authorized service account to shut down or restart the domain controller.
Allow to eject removable NTFS media	Not defined	Administrators	Allows only Administrators to eject removable NTFS media to protect against the theft of sensitive data.
Amount of idle time required before disconnecting session	Not defined	15 minutes	Controls when a domain controller suspends an inactive server message block (SMB) session, which has no security implications but which reduces SMB traffic resource usage.
Audit the access of global system objects	Not defined	Disabled	Disables the creation of a default SACL on system objects, such as mutexes(mutual exclusive), events, semaphores, and DOS devices because the default policy is “No auditing.”
Audit use of Backup and Restore privilege	Not defined	Disabled	Disables auditing for the use of user privileges, including Backup and Restore, when the “Audit privilege use” policy is enabled because this policy is configured for “No auditing.”
Automatically log off users when logon time expires	Not defined	Enabled	Forcibly disconnects client sessions with the SMB Service when the user’s logon hours expire to ensure that network connections are secured during nonworking hours.
Automatically log off users when logon time expires (local)	Not defined	Enabled	Forcibly logs off users with interactive sessions when the user’s logon hours expire to ensure that network connections are secured during nonworking hours.
Clear virtual memory pagefile when system	Not defined	Enabled	Eliminates process memory data from going into the pagefile on

shuts down			shutdown in case an unauthorized user manages to directly access the pagefile.
Digitally sign client communication (always)	Not defined	As per requirement	See in case mixed operating systems are deployed
Digitally sign client communication (when possible)	Not defined	As per requirement	See in case mixed operating systems are deployed
Digitally sign server communication (always)	Not defined	As per requirement	See in case mixed operating systems are deployed
Digitally sign server communication (when possible)	Enabled	(No change)	See in case mixed operating systems are deployed
Disable CTRL + ALT + DEL requirement for logon	Not defined	Disabled	Requires CTRL+ALT+DEL before users log on to ensure that users are communicating by means of a trusted path when entering their passwords.
Do not display last user name in logon screen	Not defined	Enabled	Removes the name of the last user to successfully log off from the Log On to Windows dialog box to prevent attackers from discovering service account names on domain controllers.
LAN Manager Authentication Level	Not defined	(See comments)	See in case mixed operating systems are deployed
Message text for users attempting to log on	Not defined	As per requirement	May provide some sort of warning and undertaking message for users attempting to logon
Message title for users attempting to log on	Not defined	(No change)	
Number of previous logons to cache (in case domain controller is not available)	Not defined	0 logons	The value 0 indicates that the domain controller does not cache previous logons and requires authentication at each logon.
Prevent system maintenance of computer account password	Not defined	Disabled	Not enabled because computer account passwords are used to establish secure channel communications between members and domain controllers and, within the domain, between the domain controllers themselves. After it is established, the secure channel is used to transmit sensitive information that is necessary for making authentication and authorization

			decisions.
Prevent users from installing printer drivers	Not defined	Enabled	Allows only Administrators and Server Operators to install a printer driver when adding a network printer to ensure that users cannot install a printer driver (add a network printer) and perform disk-space attacks by submitting large print jobs.
Prompt user to change password before expiration	Not defined	14 days	Notifies users in advance (in days) that their password is about to expire so that the user has time to construct a password that is sufficiently strong.
Recovery Console: Allow automatic administrative logon	Not defined	Disabled	Requires that an Administrator account password must be given before access is granted to a domain controller to ensure that anyone logging on requires administrator credentials.
Recovery Console: Allow floppy copy and access to all drivers and all folders	Not defined	Disabled	Prevents unauthorized users from gaining access to, copying, and removing the Active Directory database and other secure files from the domain controller.
Rename administrator account	Not defined	(No change)	
Rename guest account	Not defined	(No change)	
Restrict CD-ROM access to locally logged-on users only	Not defined	Enabled	Allows only the interactively logged-on service administrator to access removable CD-ROM media to ensure that when no one is logged on interactively, the CD-ROM cannot be accessed over the network.
Restrict floppy access to locally logged-on users only	Not defined	Enabled	Allows only interactively logged-on service administrators to access removable floppy media to ensure that the floppy cannot be accessed over the network when no one is logged on.
Secure channel: Digitally encrypt or sign secure channel data (always)	Not defined	Enabled	Requires Windows NT 4.0 with Service Pack 6 or newer software on all domain controllers in local and all trusted domains to ensure that all security fixes have been made.
Secure channel:	Not defined	(No change)	

Digitally encrypt secure channel data (when possible)			
Secure channel: Digitally sign secure channel data (when possible)	Not defined	(No change)	
Secure channel: Require strong (Windows 2000 or later) session key	Not defined	Enabled	Requires that a secure channel be established with 128-bit encryption to ensure that the key strength is not negotiated but always uses the most secure connection possible with the domain controller.
Secure system partition (for RISC platforms only)	Not defined	(No change)	
Send unencrypted password to connect to third-party SMB servers	Not defined	Disabled	Prohibits the SMB redirector from sending plaintext passwords to non-Microsoft SMB servers that do not support password encryption. Disable this policy unless your domain controller needs to communicate with non-Microsoft SMB servers.
Shut down system immediately if unable to log security audits	Not defined	Disabled	Stops the domain controller if a security audit cannot be logged. The auditing goals for domain controllers, in “Establishing Domain Controller Audit Policy Settings” allow overwriting Security audit events as required.
Smart card removal behavior	Not defined	Force logoff	Forces service administrators to keep smart cards inserted while logged on interactively on domain controllers to ensure that domain controllers are not left logged on to and unattended.
Strengthen default permissions of global system objects (e.g. Symbolic Links)	Not defined	Enabled	Allows users who are not administrators to read shared objects but not modify them. Strengthens the default DACL of objects in the global list of shared resources, such as DOS device names, mutexes, and semaphores.
Unsigned driver installation behavior	Not defined	Do not allow installation	Prevents insecure or untrusted device drivers from being installed

			on domain controllers.
Unsigned non-driver installation behavior	Not defined	Silently succeed	Nondriver signing was not implemented in most software applications and services. Policy has no real benefit and is set to eliminate unnecessary notification.

3.3.4 Establish Domain Controller Event Log Policy Settings

When domain controller audit policy is enabled, the maximum size of the security log should also be increased to accommodate the increased number of audited events that would be generated. The event log policy settings recommended here reflect the changes that are necessary to support the recommended audit policy.

Policy	Default Setting	Recommended Setting	Comments
Maximum application log size	Not defined	(No change)	
Maximum security log size	Not defined	128 MB	Increased to accommodate security auditing that is enabled in the domain controller audit policies.
Maximum system log size	Not defined	(No change)	
Prevent local guests group from accessing application log	Not defined	Enabled	Prevents members of the built-in group Guests from reading the application log events.
Prevent local guests group from accessing security log	Not defined	Enabled	Prevents members of the built-in group Guests from reading the security log events.
Prevent local guests group from accessing system log	Not defined	Enabled	Prevents members of the built-in group Guests from reading the system log events.
Retain application log	Not defined	(No change)	
Retain security log	Not defined	(No change)	
Retain system log	Not defined	(No change)	
Retention method for application log	Not defined	(No change)	
Retention method for security log	Not defined	Overwrite events as needed	Overwrites the security log when the maximum log size is reached to ensure that the log contains the most recent security events and to

			ensure that logging continues.
Retention method for system log	Not defined	Overwrite events as needed	Overwrites the system log when the maximum log size is reached to ensure that the log contains the most recent security events and to ensure that logging continues.
Shutdown the computer when the security audit log is full	Not defined	(No change)	

3.4 Services

Only required services should be started on the server. All the unnecessary services should be disabled or set accordingly. The recommended Services to Install on a Windows 2000 Server are explained below.

Service Name	**Default Startup Type**	**Recomme nded Startup Type**	**Comment**
Alerter	Automatic	(No change)	Notifies selected users and computers of administrative alerts.
Application Management	Manual		Provides software installation services for applications that are deployed through Add/Remote Programs. On dedicated domain controllers, this service can be disabled to prevent unauthorized installation of software.
Automatic Updates	Manual		Provides the download and installation of critical Windows updates, such as security patches or hotfixes.
Background Intelligent Transfer Service	Manual		Provides a background file transfer mechanism and queue management, and it is used by Automatic Update to automatically download programs (such as security patches). This service can be disabled when automatic updates are not performed on the domain controller. It is included when SP3 is applied.
ClipBook	Manual		Enables the Clipbook Viewer to create and share “pages” of data to be reviewed by remote users. On dedicated domain controllers, this

			service can be disabled.
COM+ Event System	Manual	(No change)	Provides automatic distribution of events to COM components.
Computer Browser	Automatic	(No change)	Maintains the list of computers on the network, and supplies the list to programs that request the list.

Service Name	Default Startup Type	Recommended Startup Type	Comment
DHCP Client	Disabled	(No change)	
Distributed File System	Automatic	(No change)	Manages logical volumes that are distributed across a local area network (LAN) or wide area network (WAN), and it is required for the Active Directory SYSVOL share.
Distributed Link Tracking Client	Automatic	Disabled	Maintains links between NTFS v5 file system files within the domain controllers and other servers in the domain. Disable Distributed Link Tracking Client on dedicated domain controllers.
Distributed Link Tracking Server	Manual	Disabled	Tracks information about files that are moved between NTFS v5 volumes throughout a domain. Disable Distributed Link Tracking Server on dedicated domain controllers.
DNS Client	Automatic	(No change)	Allows resolution of DNS names.
DNS Server	Automatic	(No change)	Required for Active Directory–integrated DNS zones.
Event Log	Automatic	(No change)	Writes event log messages that are issued by Windows-based programs and components to the log files.
Fax Service	Manual	Disabled	Provides the ability to send and receive faxes through fax resources that are available on the domain controller and network. On dedicated domain controllers, this service can be disabled because sending and receiving faxes is not a normal function of a domain controller.
File Replication Service	Manual	(No change)	Enables files to be automatically copied and maintained simultaneously on multiple computers, and it is used to replicate SYSVOL among all domain controllers.

Indexing Service	Manual		Indexes content and properties of files on the domain controller to provide rapid access to the file through a flexible querying language. On dedicated domain controllers, disable this service to prevent users from searching files and file content if sensitive files and folders are inadvertently indexed.
Internet Connection Sharing	Manual	Disabled	Provides network address translation (NAT), addressing and name resolution, and intrusion detection when connected through a dial-up or broadband connection. On dedicated domain controllers, disable to prevent inadvertent enabling of NAT, which would prevent the domain controller from communicating with the remainder of the network.
Intersite Messaging	Disabled	(No changes)	Required by SMTP replication in Active Directory, DFS, and NETLOGON.
IPSEC Policy Agent	Automatic	(No change)	Provides management and coordination of Internet Protocol Security (IPSec) policies with the IPSec driver.
Kerberos Key Distribution enter	Disabled	(No change)	Provides the ability for users to log on using the Kerberos V5 authentication protocol.
License Logging Service	Automatic		Monitors and records client access licensing for portions of the operating system, such as IIS, Terminal Services, and file and print sharing, and for products that are not a part of the operating system, such as Microsoft SQL Server or Microsoft Exchange Server. On a dedicated domain controller, this service can be disabled.
Logical Disk Manager	Automatic	(No change)	Required to ensure that dynamic disk information is up to date.
Logical Disk Manager Administrative Service	Manual	(No change)	Required to perform disk administration.
Messenger	Automatic	(No change)	Transmits net sends and Alerter service messages between clients

			and servers.
Net Logon	Manual	(No change)	Maintains a secure channel between the domain controller, other domain controllers, member servers, and workstations in the same domain and trusting domains.
NetMeeting Remote Desktop Sharing	Manual	Disabled	Eliminates potential security threat by allowing domain controller remote administration through NetMeeting.
Network Connections	Manual	(No change)	Manages objects in the Network Connections folder.
Network DDE	Manual		Provides network transport and security for Dynamic Data Exchange (DDE) for programs running on the domain controller. This service can be disabled when no DDE applications are running locally on the domain controller.
Network DDE DSDM	Manual		Used by Network DDE. This service can be disabled when Network DDE is disabled.
NTLM Security Support Provider	Manual	(No change)	Provides security to RPC programs that use transports other than named pipes, and enables users to log on using the NTLM authentication protocol.
Performance Logs and Alerts	Manual		Collects performance data for the domain controller, writes the data to a log, or generates alerts. This service can be set to automatic when you want to log performance data or generate alerts without an administrator being logged on.
Plug and Play	Automatic	(No change)	Required to automatically recognize and adapt to changes in the domain controller hardware with little or no user input.
Print Spooler	Automatic		Manages all local and network print queues and controls all print jobs. Can be disabled on dedicated domain controllers where no printing is required.
Protected Storage	Automatic	(No change)	Protects storage of sensitive information, such as private keys, and prevents access by unauthorized services, processes, or users. This service is used on domain controllers for smart card

			logon.
QoS RSVP	Manual		Provides support for QoS RSVP routing information. This service an be disabled when QoS is not used to allocate network bandwidth in network infrastructure.
Remote Access Auto Connection Manager	Manual		Detects unsuccessful attempts to connect to a remote network or computer and provides alternative methods for connection. This service can be disabled on dedicated domain controllers where no virtual private network (VPN) or dial-up connections are initiated.
Remote Access Connection Manager	Manual		Manages VPN and dial-up connection from the domain controller to the Internet or other remote networks. This service can be disabled on dedicated domain controllers where no VPN or dial-up connections are initiated.
Remote Procedure Call (RPC)	Manual	(No change)	Serves as the RPC endpoint mapper for all applications and services that use RPC communications.
Remote Procedure Call (RPC) Locater	Automatic		Enables RPC clients using the RpcNs* family of application programming interfaces (APIs) to locate RPC servers and manage the RPC name service database. This service can be disabled if no applications use the RpcNs* APIs.
Remote Registry Service	Automatic	(No change)	Enables remote users to modify registry settings on the domain controller, provided the remote users have the required permissions. By default, only Administrators and Backup Operators can access the registry remotely.
Removable Storage	Automatic		Manages and catalogs removable media, and operates automated removable media devices, such as tape auto loaders or CD jukeboxes. This service can be disabled when removable media devices are directly connected to the domain controller.
Routing and Remote Access	Disabled	(No change)	Enables LAN-to-LAN, LAN-to-WAN, VPN, and NAT routing services.

RunAs Service	Automatic	(No change)	Allows you to run specific tools and programs with different privileges than your current logon provides.
Security Accounts Manager	Automatic	(No change)	A protected subsystem that manages user and group account information.
Server	Automatic	(No change)	Provides RPC support, file print, and named pipe sharing over the network.
Smart Card	Manual	(No change)	Manages and controls access to a smart card that is inserted into a smart card reader attached to the domain controller.
Smart Card Helper	Manual	(No change)	Provides support for legacy, non-plug-and-play smart card readers.
System Event Notification	Automatic	(No change)	Monitors system events and notifies subscribers to the COM+ Event System of these events.
Task Scheduler	Automatic	(No change)	Provides the ability to schedule automated tasks on the domain controller.
TCP/IP NetBIOS Helper Service	Automatic	(No change)	Provides support for the NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution for clients.
Telephony	Manual		Provides Telephony API (TAPI) support of client programs that control telephony devices and IP-based voice connections. This service can be disabled on dedicated domain controllers where TAPI is not used by applications.
Telnet	Manual	Disabled	Enables a remote user to log on and run applications from a command line on the domain controller. Enable Telnet only when it is used for remote administration for branch offices or headless domain controllers. Terminal Services is the recommended method for remote administration.
Terminal Services	Disabled		Allows multiple remote users to be connected interactively to the domain controller, and provides display of desktops and run applications. To reduce the surface area of attack, disable Terminal Services unless it is used for remote administration for branch offices or

			headless domain controllers.
Uninterruptible Power Supply	Automatic	(No change)	Manages an uninterruptible power supply (UPS) that is connected to the domain controller by a serial port.
Utility Manager	Manual	Disabled	Allows faster access to some accessibility tools, such as Magnifier, Narrator, and On-Screen Keyboard, and also displays the status of the tools or devices that it controls. Disable Utility Manager unless you require these special accessibility tools.
Windows Installer	Manual	(No change)	Adds, modifies, and removes applications that are provided as a Windows Installer (.MSI) package.
Windows Management Instrumentation	Manual	(No change)	Provides a common interface and object model to access management information about the domain controller through the WMI interface.
Windows Management Instrumentation Drivers	Manual	(No change)	Monitors all drivers and event trace providers that are configured to publish WMI or event trace information.
Windows Time	Manual	(No change)	Sets the domain controller clock, and maintains date and time synchronization on all computers in the network.
Workstation	Automatic	(No change)	Creates and maintains client network connections to remote servers.

The antivirus software installed on the server run as a service. The default configuration of antivirus software should not be changed.

The following Table lists the changes to the service startup configuration when a server running Windows 2000 is promoted to a domain controller. This table is provided as a reference, to arrive at the final list of services to have running on a domain controller.

Service Name	**Default Startup Type**	**Recommended Startup Type**	**Comment**
Distributed Link Tracking Server	Automatic	Disabled	Tracks information about files that are moved between NTFS v5 volumes throughout a domain. Disable Distributed Link Tracking Server on dedicated domain controllers.

File Replication Service	Automatic	(No change)	Enables files to be automatically copied and maintained simultaneously on multiple computers. This service is used to replicate SYSVOL between all domain controllers.
Intersite Messaging	Automatic	(No changes)	Required by SMTP replication in Active Directory, DFS, and NETLOGON.
Kerberos Key Distribution enter	Automatic	(No change)	Provides the ability for users to log on using the Kerberos V5 authentication protocol.
Net Logon	Automatic	(No change)	Maintains a secure channel between the domain controller, other domain controllers, member servers, and workstations in the same domain and in trusting domains.
Remote Procedure Call (RPC) Locater	Automatic		Enables RPC clients using the RpcNs* family of APIs to locate RPC servers and manage the RPC name service database. This service can be disabled if no applications use the RpcNs* APIs.
Windows Management Instrumentation	Automatic	(No change)	Provides a common interface and object model to access management information about the domain controller through the WMI interface.
Windows Time	Automatic	(No change)	Sets the domain controller clock, and maintains date and time synchronization on all computers in the network.

3.5 Vulnerability Scanning Tools

After applying security settings to the server, vulnerability scanning Tools like Retina, Look@LAN, ISS, Shadow etc. should be used. Any vulnerability found by these tools should immediately be fixed.

4. Incident Handling

SA should prepare the system for handling an incident. While the actions outlined in this guideline will dramatically increase system security, system vulnerabilities may exist. New security holes are discovered regularly, thus, preparing for the worst is critical. These steps should help to facilitate identifying a system compromise, allow for forensic analysis, and enable a timely recovery.

4.1 Identifying a System Compromise

Aside from consistently watching for common indications of a system compromise (listed below), SA should consider recording cryptographic checksums. By doing so one can establish a baseline of system binaries, application code, and data. This allows SA to compare the current file system against a known reliable version.

- A system alarm or similar indication from an intrusion detection tool
- Suspicious entries in system or network accounting
- Accounting discrepancies
- Unsuccessful logon attempts
- New user accounts of unknown origin
- New files of unknown origin and function
- Unexplained changes or attempt to change file sizes, check sums, date/time stamps, especially those related to system binaries or configuration files
- Unexplained addition, deletion, or modification of data
- Denial of service activity or inability of one or more users to login to an account; including admin/root logins to the console
- System crashes
- Poor system performance
- Unauthorized operation of a program or the addition of a sniffer application to capture network traffic or usernames/passwords
- Port Scanning (use of exploit and vulnerability scanners, remote requests for information about systems and/or users, or social engineering attempts)
- Unusual usage times (statistically, more security incidents occur during non-working hours than any other time)
- An indicated last time of usage of a account that does not correspond to the actual last time of usage for that account
- Unusual usage patterns (e.g., programs are being compiled in the account of a user who does not know how to program)

The most commonly accepted cryptographic checksum used is the MD5 algorithm.

4.2 Forensic Analysis

Forensic Analysis is the process of unearthing data of probative value from computer and information systems. Thus, it is imperative to maintain the integrity of possible evidence. This includes log files, trusted cryptographic checksums, and information pertaining to system users/groups.

Hackers are ever increasing an ability to cover their trails. Log files are often deleted or modified to protect the identity of the intruder. Thus, measures to preserve the integrity of log files should be taken. Perhaps the best method is to use a remote logging software application that allows system logs to be stored on a remote system. The following list of actions will greatly increase the ability for investigators to pursue an intruder.

- Set proper permissions on log files
- Use a separate server to gather log files
- Make regular backups of log files
- Use write once media for log files
- Encrypt the log files
- Review log files on a frequent basis

4.3 Timely Recovery

Regular complete system backups can be a useful resource during the recovery process. Using commercial software such as Ghost allows creating a production image of the system after service packs, hotfixes, and security settings have been applied. This allows rebuilding the system to a trusted version of the system configuration quickly. Traditional backup methods are also useful for protecting applications and data.

4.4 Incident reporting

All Security Incidents should be informed to CERT-In, at http://www.cert-in.org.in

5. References

1. Microsoft Best Practice Guide for Securing Active Directory Installations and Day-to-Day Operations
   http://www.microsoft.com

2. NIST Systems Administration Guidance for Securing Windows 2000 Professional Systems
   http://www.nist.org

3. The Centre for Internet Security Windows 2000 Server Operating System Lavel2 Benchmark Consensus Baseline Security Settings
   http://www.cisecurity.org

4. Microsoft TechNet Knowledgebase Articles
   http://support.microsoft.com

Appendix A

Registry Settings

Suppress Dr. Watson Crash Dumps: **HKLM\Software\Microsoft\DrWatson\CreateCrashDump (REG_DWORD) 0**

Disable Automatic Execution of the System Debugger: **HKLM\Software\Microsoft\Windows NT\CurrentVersion\AEDebug\Auto (REG_DWORD) 0**

Disable autoplay from any disk type, regardless of application: **HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun (REG_DWORD) 255**

Disable autoplay for the current user: **HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun (REG_DWORD) 255**

Disable autoplay for new users by default: **HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun (REG_DWORD) 255**

Disable Automatic Logon: **HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AutoAdminLogon (REG_DWORD) 0**

Mask any typed passwords with asterisks: **HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Network\HideSharePwds (REG_DWORD) 1**

Disable Dial-in access to the server: **HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Network\ NoDialIn (REG_DWORD) 1**

Disable automatic reboots after a Blue Screen of Death: **HKLM\System\CurrentControlSet\Control\CrashControl\AutoReboot (REG_DWORD) 0**

Disable CD Autorun: **HKLM\System\CurrentControlSet\Services\CDrom\Autorun (REG_DWORD) 0**

Remove administrative shares on servers: **HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareServer (REG_DWORD) 0**

Protect against Computer Browser Spoofing Attacks: **HKLM\System\CurrentControlSet\Services\MrxSmb\Parameters\RefuseReset (REG_DWORD) 1**

Protect against source-routing spoofing: **HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting (REG_DWORD) 2**

Protect the Default Gateway network setting: **HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect (REG_DWORD) 0**

Ensure ICMP Routing via shortest path first: **HKLM\System\ CurrentControlSet\Services\Tcpip\ Parameters\EnableICMPRedirect (REG_DWORD) 0**

Help protect against packet fragmentation: **HKLM\System\CurrentControlSet\ Services\Tcpip\Parameters\EnablePMTUDiscovery (REG_DWORD) 1**

Manage Keep-alive times: **HKLM\System\CurrentControlSet\Services\Tcpip\ Parameters\KeepAliveTime (REG_DWORD) 300000**

Protect Against Malicious Name-Release Attacks: **HKLM\System\ CurrentControlSet\Services\Netbt\Parameters\NoNameReleaseOnDemand (REG_DWORD) 1**

Ensure Router Discovery is Disabled: **HKLM\System\CurrentControlSet\ Services\Tcpip\Parameters\PerformRouterDiscovery (REG_DWORD) 0**

Protect against SYN Flood attacks: **HKLM\System\CurrentControlSet\ Services\Tcpip\Parameters\SynAttackProtect (REG_DWORD) 2**

SYN Attack protection – Manage TCP Maximum half-open sockets: **HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\ TcpMaxHalfOpen (REG_DWORD) 100 or 500**

SYN Attack protection – Manage TCP Maximum half-open retired sockets: **HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\ TcpMaxHalfOpenRetired (REG_DWORD) 80 or 400**

Enable IPSec to protect Kerberos RSVP Traffic: **HKLM\System\ CurrentControlSet\Services\IPSEC\NoDefaultExempt (REG_DWORD) 1**

Appendix B

Security Resources

http://www.cert.org
http://www.auscert.org
http://www.singcert.sg.org
http://www.securityfocus.org
http://web.mit.edu/kerberos/www/
http://windows2000.about.com/cs/security/
http://windowsupdate.microsoft.com/
http://is-it-true.org/nt/nt2000/
http://microsoft.com/windows/ie/evaluation/overview/privacy.asp
http://msdn.microsoft.com
http://www.activewin.com/win2000/index.shtml